Universidade de Aveiro Departamento de Matemática,
2013

Francisco Santos Teixeira Pires

Representação dos números na forma decimal e generalização a outras bases

Francisco Santos Teixeira Pires

Representação dos números na forma decimal e generalização a outras bases

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Matemática para Professores realizada sob a orientação científica do Professor Doutor Paulo José Fernandes Almeida, Professor Auxiliar do Departamento de Matemática da Universidade de Aveiro.

o júri / the jury

presidente / president

Professora Doutora Andreia Oliveira Hall
Professora Associada do Departamento de Matemática da Universidade de Aveiro

vogais / examiners committee

Professor Doutor Luís Filipe dos Santos Roçadas Ferreira
Professor Auxiliar do Departamento de Matemática da Escola de Ciências e Tecnologias da Universidade de Trás-os-Montes e Alto Douro

Professor Doutor Paulo José Fernandes Almeida
Professor Auxiliar do Departamento de Matemática da Universidade de Aveiro (orientador)

agradecimentos / acknowledgements

A Deus por me sustentar nos momentos difíceis e suprir todas as minhas necessidades.

À minha linda família, esposa e filhos, pelo carinho, paciência e incentivo.

Ao Professor Doutor Paulo José Fernandes Almeida, pelo entusiasmo e amizade com que sempre me transmitiu os ensinamentos, sugestões e críticas, pela atenção e enorme disponibilidade.

Palavras-chave representação numérica, número racional, dízima finita, dízima infinita periódica, período, comprimento do período, teorema de Midy, números parasíticos, números cíclicos, números n-cíclicos, critérios de divisibilidade, adição-Nim

Resumo Qualquer número racional pode ser representado por uma dízima finita ou uma dízima infinita periódica. Porém, atendendo ao denominador de uma fração que representa o número racional, podemos obter diversos períodos diferentes. Neste sentido, destacamos um resultado importante que nos possibilita a determinação do comprimento do período de uma dízima. Com base nessa noção de período, evidenciamos o fascinante teorema de Midy. Abordamos, ainda, alguns critérios de divisibilidade por números primos associados à representação de números. Estudamos, também, os números *teimosos* que quando multiplicados por um certo valor sofrem apenas uma alteração posicional dos seus algarismos. Mostramos como se pode utilizar a operação aritmética especial, a adição-Nim, na obtenção de uma estratégia vencedora para jogos combinatórios.

Keywords numerical representation, rational number, finite decimal, repeating decimal, period, length of the period, theorem of Midy, parasitic number, ciclic number, n-cilic number, divisibility criteria, Nim-addition

Abstract Any rational number can be represented by a finite or repeating decimal. However, depending on the denominator of the fraction that represents the rational number, one can obtain many different periods. On this regard, we highlight an important result that allows us to determine the length of the period of a repeating decimal. Based on this notion of period, we study the fascinating theorem of Midy. We also study the stubborn numbers, which when multiplied by a certain value suffer just a positional change of its digits. Moreover, some divisibility criteria by prime numbers will be investigated the representation of numbers. We also show how one can use the special arithmetic operation, known as nim addiction, to obtain winning strategy for combinatorial games.

"Deus criou os números (inteiros); tudo o resto é obra do Homem."

– *Leopold Kronecker*

Conteúdo

Capítulo 1

Preliminares

1.1 Introdução

Com esta dissertação pretendemos estudar a representação de números, utilizando o sistema numérico decimal e, ainda, procurando a generalização a outros sistemas numéricos. Importa salientar que o capítulo 9 do Hardy e Wright (ver [15]) constitui uma referência no estudo dos diversos conceitos e resultados a apresentar. Com efeito, a riqueza adicional das frações, na promoção da descoberta de inter-relações numéricas e a exploração de jogos combinatórios, cujo estudo levou à abordagem de uma operação aritmética especial que permitiu determinar quais as posições de jogo que se deve tentar obter para vencer o jogo, constituem temáticas estruturantes do texto a desenvolver.

O sistema numérico decimal é um sistema posicional de representação que parte dos algarismos 0 a 9 e cria outros números a partir de adições e multiplicações. Qualquer símbolo que é posicionado à direita de outro implica multiplicar esse outro por uma potência de 10 maior do que aquela que esse símbolo é multiplicado.

O sistema decimal utiliza a base 10, assim, na passagem da unidade, para a dezena, centena, milhar, em diante, utilizamos as potências de 10. Por exemplo, tomemos o numeral 688 que representa o número seiscentos e oitenta e oito. O algarismo 8 tem valor posicional 8 na primeira posição e valor posicional 80 na segunda posição. O símbolo 0, zero, serve para representar uma posição vazia no número, que pode ser a ausência de unidades, de dezenas, de centenas, etc. O sistema decimal é multiplicativo, pois cada numeral representa o produto dele mesmo pelo valor da posição que ocupa, assim como, é também aditivo, uma vez que o numeral representa um número que é a soma dos valores posicionais de cada algarismo.

Neste texto concentramo-nos nos números que podem ser representados por *frações* do tipo $\frac{1}{3}, \frac{2}{7}, \ldots$, isto é, ao quociente entre quaisquer dois números inteiros (exceto quando

o divisor é zero), a que chamamos números racionais. Qualquer número racional pode ser representado por uma dízima finita ou por uma dízima infinita periódica. Este resultado vem acicatar-nos a procura de respostas acerca de determinadas curiosidades, como, por exemplo: Qual a dimensão do período de uma dízima infinita períodica?

Embrenhados, ainda mais, na noção de período exploramos um resultado fascinante que é o Teorema de Midy.

Não menos interessante será conhecer alguns números que designamos por números *teimosos*, pois quando multiplicados por um certo valor sofrem apenas uma alteração posicional dos seus algarismos.

No prosseguimento desta dissertação, desenvolve-se, ainda, o estudo pela procura da melhor estratégia de *como ganhar no momento certo* ante alguns jogos combinatórios.

Assim, o presente texto encontra-se organizado da seguinte forma:

No capítulo inicial e, para melhor compreendermos o trabalho desenvolvido nesta dissertação, revemos alguns conceitos de Teoria de Números.

No capítulo dois, vamos estudar a *mais-valia* que nos concede as dízimas, nomeadamente a representação de números por uma dízima e a noção de período de uma dízima. No desenvolvimento desta última noção, salienta-se o teorema de Euler na determinação do comprimento do período de uma dízima infinita periódica. A exploração, ainda, deste conceito conduz-nos a um resultado extraordinário, ao *Teorema de Midy* e, também, à sua generalização. Por fim, exploramos algumas relações que o conjunto dos coeficientes de uma representação numérica concede no estabelecimento de critérios de divisibilidade por números primos.

No capítulo três, vamos estudar alguns números notáveis, designadamente os números parasíticos e os números cíclicos. No que concerne aos primeiros, estes têm a particularidade de se agarrarem como os *parasitas*, no sentido em que quando multiplicados por um certo valor, obtém-se um número que sofreu apenas uma rotação dos seus algarismos, ou seja, o algarismo mais à direita da sua representação numérica altera-se para a frente, enquanto os números cíclicos têm a característica de quando multiplicados por determinado valor, obtém-se um número cujos algarismos formam permutações cíclicas dos algarismos desses números. De notar que estes conceitos serão objeto de estudo noutras bases numéricas diferentes da base 10.

No último capítulo desta dissertação, o capítulo quatro, destacamos uma operação aritmética especial, que designamos por adição-Nim, em contexto de jogos combinatórios, onde toma a função central no desenvolvimento estratégico de jogadas vencedoras. Esta operação consubstancia-se em "regras", definidas diferentes das habituais, que se estabelecem a partir da representação numérica binária.

1.2 Conceitos de Teoria dos Números

Importa salientar que o desenvolvimento desta secção teve por base as notas escritas pelo Professor Doutor Paulo Almeida (ver [1]) para a disciplina de Teoria de Números.

Nesta secção introduzimos alguns conceitos e resultados fundamentais nos quais se baseiam inúmeros assuntos abordados ao longo desta dissertação. Deste modo, iniciamos o nosso estudo com a introdução de uma das noções importantes para o estudo dos números.

Definição 1.2.1 (Divisibilidade). *Sejam a e b dois inteiros. Se $a \neq 0$ e existir um inteiro c tal que $b = ac$, dizemos que a* divide *b, e escrevemos $a|b$. Se a* não divide *b, escrevemos $a \nmid b$.*

Atendendo a esta definição, verificamos que qualquer número inteiro admite divisores positivos e negativos. No entanto, e uma vez que para estes últimos é dada pouca importância no contexto dos conceitos e/ou resultados a estudar, sendo o estudo similar, de agora em diante fazemos apenas referência aos números inteiros positivos.

A noção de divisibilidade introduzida na definição 1.2.1 está na base de algumas propriedades básicas de grande importância, verificadas pelos números inteiros, de entre as quais, por nos serem úteis ao longo deste texto, destacamos:

1. Se $a|b$ verifica-se $a|cb$, para qualquer inteiro c;
2. Se $a|b$ e $b|b'$ verifica-se $a|b'$;
3. Se $a|b$ e $a|b'$ então $a|(mb + nb')$, para quaisquer inteiros m e n.

Alguns inteiros positivos, como 2, 3, 5, 7, 11 e 17, só são divisíveis por eles próprios e por 1. Estes números são chamados *números primos*. Assim, a definição de um número primo é a seguinte:

Definição 1.2.2 (Números primos e Números compostos). *A qualquer inteiro maior que* 1*, cujos únicos divisores positivos sejam ele próprio e* 1*, chamamos* número primo. *Um inteiro maior que* 1 *que não seja primo é um* número composto.

É sabido que o estudo dos números primos 2, 3, 5, 7, 11, 13 . . . constitui um assunto de grande interesse na Teoria dos Números. Também, ao longo desta dissertação estes números assumem um papel relevante no estudo de resultados importantes. Contudo, importa ainda introduzirmos outro conceito adicional, que nos permite calcular o maior número inteiro positivo que divide simultaneamente dois quaisquer inteiros a e b que conheçamos.

Definição 1.2.3 (Máximo divisor comum). *Sejam a e b dois inteiros tais que pelo menos um deles é não nulo. Chamamos* máximo divisor comum *ao maior elemento do conjunto dos divisores comuns de a e b e designamos este elemento por (a, b).*

Consequentemente, a noção de *máximo divisor comum* leva-nos a um outro conceito fundamental.

Definição 1.2.4 (Números primos entre si). *Sejam a e b inteiros e pelo menos um deles é não nulo. Se $(a, b) = 1$ então dizemos que a e b são* primos entre si.

Debrucemo-nos sobre a forma como podemos determinar o máximo divisor comum entre dois inteiros a e b não simultaneamente nulos. A este processo chamamos algoritmo de Euclides. Assim, através do algoritmo da divisão, podemos obter dois inteiros q_0 e r_0, tais que

$$a = q_0 b + r_0, \quad \text{com} \quad 0 \leq r_0 < b.$$

Se $r_0 \neq 0$ podemos utilizar o algoritmo da divisão para os inteiros b e r_0. Então existem q_1 e r_1 tais que

$$b = q_1 r_0 + r_1, \quad \text{com} \quad 0 \leq r_1 < r_0.$$

Continuando desta forma, ou seja, procedendo à divisão de um resto pelo seguinte (denotando b por r_{-1} e a por r_{-2}) divide-se o resto i pelo resto $i + 1$, com $-2 \leq i \leq k - 1$. O último resto não nulo, r_k, vai ser o máximo divisor comum entre a e b. Com efeito, obtemos uma sequência de inteiros não negativos $r_0, r_1, r_2 \ldots, r_k$, tais que $r_0 > r_1 > \cdots > r_k > 0$, pelo que o algoritmo de Euclides termina ao fim de um número finito de passos.

Teorema 1.2.5 *Se a e b são dois inteiros positivos e r_k é o último resto não nulo obtido pelo algoritmo de Euclides, então $r_k = (a, b)$. Mais, o algoritmo de Euclides permite encontrar inteiros u e v tais que*

$$au + bv = (a, b).$$

Demonstração: O algoritmo de Euclides pode ser esquematizado pelo seguinte sistema

de equações:

$$\begin{cases} a = bq_0 + r_0 \\ b = r_0q_1 + r_1 \\ r_0 = r_1q_2 + r_2 \\ \vdots \\ r_{k-2} = r_{k-1}q_k + r_k \\ r_{k-1} = r_kq_{k+1} \end{cases} \tag{1.1}$$

Seja $d = (a, b)$. Vamos provar por indução que $d \mid r_{i+1}$, para qualquer $0 \leq i \leq k-1$. Como $d|a$ e $d|b$, temos $d|(a - bq_0)$, i.e., $d|r_0$. Como $d|b$ e $d|r_0$ então $d|(b - r_0q_1) = r_1$. Agora, suponhamos que $d|r_i$ e $d|r_{i+1}$, queremos provar que $d|r_{i+2}$, onde $0 \leq i \leq k-2$. Usando a hipótese de indução, obtemos que $d|(r_i - r_{i+1}q_{i+2})$. Mas $r_i - r_{i+1}q_{i+2} = r_{i+2}$. Portanto $d|r_{i+2}$.

Acabámos de provar que $d|r_i$ para todo $0 \leq i \leq k$. Em particular, $d|r_k$. Como $d, r_k > 0$, temos $d \leq r_k$.

Reciprocamente, a última equação em (1.1) e o facto de $r_k \neq 0$, diz-nos que $r_k|r_{k-1}$. Usando a penúltima equação, obtemos $r_k|r_{k-2}$. Por indução, concluímos que $r_k|r_i$, para qualquer $0 \leq i \leq k$. Usando a segunda equação, temos $r_k|b$ e usando a primeira, $r_k|a$. Logo, $r_k|d$. Portanto, $r_k = d$.

Agora, provamos a segunda parte do teorema. Seja $r_{-2} = a$ e $r_{-1} = b$. Sabemos que

$$r_i = r_{i-2} - r_{i-1}q_i, \tag{1.2}$$

para qualquer $0 \leq i \leq k$. Vamos provar por indução que, para qualquer $0 \leq i \leq k$, existem inteiros u_i e v_i tais que $r_i = u_ia + v_ib$. Como $r_0 = a - bq_0$, o resultado é válido para $i = 0$, bem como $r_1 = b - r_0q_1$ o que mostra que também é válido para $i = 1$. Suponhamos, por hipótese de indução, que o resultado é verdadeiro para i e para $i-1$. Então

$$\begin{aligned} r_{i+1} &= r_{i-1} - r_iq_{i+1} \\ &= u_{i-1}a + v_{i-1}b - (u_ia + v_ib)q_{i+1} \\ &= (u_{i-1} - u_iq_{i+1})a + (v_{i-1} - v_iq_{i+1})b \\ &= u_{i+1}a + v_{i+1}b. \end{aligned}$$

Portanto, para qualquer $0 \leq i \leq k$, $r_i = u_ia + v_ib$. Em particular, existem inteiros u e v, tais que $r_k = ua + vb$. □

Observemos, ainda, um resultado auxiliar em algumas temáticas desta dissertação.

Teorema 1.2.6 *Se* $(n, a) = 1$ *e* $n|ab$*, então* $n|b$*. Em particular, se* p *é primo e* $p|ab$*, então* $p|a$ *ou* $p|b$*.*

Demonstração: Pelo teorema 1.2.5, se $(n, a) = 1$ então existem inteiros u e v, tais que $nu + av = 1$, donde $nbu + abv = b$. Como $n|ab$, obtemos $n|b$. Para o caso particular apresentado, se $p|a$, está provado. Se considerarmos que $p \nmid a$, então $(a, p) = 1$ e, como acabámos de provar, $p|b$. □

Em seguida, iremos introduzir, o conceito de congruência entre dois números inteiros, conceito este que utilizamos repetidamente ao longo do texto desta dissertação. Com base neste conceito simples e algumas das suas propriedades elementares podemos demonstrar dois dos teoremas mais importantes desta secção, o teorema de Euler e o pequeno teorema de Fermat, que nos servem de base para muitos dos resultados utilizados ao longo deste texto.

Definição 1.2.7 (Congruência). *Sejam* a *e* b *inteiros e* n *um inteiro positivo. Se* $n \mid (a - b)$*, dizemos que* a *é* congruente *com* b módulo n *e escrevemos*

$$a \equiv b \mod n.$$

Atendendo à definição de divisibilidade, temos o seguinte: se $a \equiv b \mod n$ então existe um inteiro k tal que $a = b + kn$.

Na nossa vida diária usamos congruências em várias situações, como, por exemplo, os relógios de ponteiros "medem" as horas $\mod 12$ e os dias da semana "medem" os dias $\mod 7$;

O resultado que a seguir apresentamos indica-nos que as relações de congruência verificam, ainda, outras propriedades básicas importantes:

Teorema 1.2.8 *Sejam* a*,* b*,* c *e* d *inteiros. Se* $a \equiv b \mod n$ *e* $c \equiv d \mod n$ *então*

(a) $a + c \equiv b + d \mod n$*;*

(b) $a - c \equiv b - d \mod n$*;*

(c) $ac \equiv bd \mod n$*.*

Demonstração: A demonstração de (a), (b) e (c) é imediata, uma vez que, tendo em conta as propriedades da divisibilidade e a definição 1.2.7, temos:

$$a + c = (b + kn) + (d + k'n) = b + d + nk'',$$

$$a - c = (b + kn) - (d + k'n) = b - d + nk'',$$

$$ac = (b + kn)(d + k'n) = bd + bk'n + dkn + kk'n = bd + nk'''.$$

□

Introduzimos, ainda, um outro resultado importante, sobretudo no auxílio à demonstração do teorema de Euler.

Teorema 1.2.9 *Se* $(a, n) = 1$ *e* $ab \equiv ac \mod n$, *então* $b \equiv c \mod n$. *Em geral, se* $(a, n) = d$ *e* $ab \equiv ac \mod n$ *então*

$$b \equiv c \mod \frac{n}{d}.$$

Demonstração: Suponhamos que $(a, n) = d$ e $ab \equiv ac \mod n$. Então existe um inteiro k tal que $ab = ac + kn$. Sejam

$$a_1 = \frac{a}{d}, \quad n_1 = \frac{n}{d}.$$

Claramente, a_1 e n_1 são inteiros e $(a_1, n_1) = 1$. Dividindo ambos os membros de $ab = ac + kn$ por d, obtém-se $a_1(b - c) = kn_1$. Donde, $a_1 \mid kn_1$. Como $(a_1, n_1) = 1$, pelo teorema 1.2.6, $a_1|k$. Portanto, $k = a_1k_1$, para algum inteiro k_1. Assim, $b - c = k_1n_1$, ou seja $n_1 \mid (b - c)$. Logo, $b \equiv c \mod \frac{n}{d}$. □

Antes de enunciarmos os dois teoremas estruturantes, implicados na abordagem a resultados fundamentais desenvolvidos ao longo deste texto, apresentamos, ainda, dois conceitos relevantes.

Definição 1.2.10 (Sistema completo de resíduos). *Um conjunto de inteiros* $a_1, a_2, \ldots, a_n$ *diz-se um* sistema completo de resíduos $\mod n$, *se qualquer inteiro é congruente,* $\mod n$ *com um e um só* a_j, *ou seja, se para cada número inteiro* x *existe um e um só* a_j *tal que* $x \equiv a_j \mod n$.

Exemplo 1.2.11 : *Os conjuntos* $\{-3,-2,-1,0,1,2,3\}$ *e* $\{-7,8,-5,10,-3,19,13\}$ *são sistemas completos de resíduos módulo* 7.

Definição 1.2.12 (Sistema reduzido de resíduos). *Seja* S *um sistema completo de resíduos* mod n. *Ao conjunto* T *formado pelos membros de* S *que são primos com* n *chamamos* sistema reduzido de resíduos mod n.

Em seguida iremos definir a função de Euler, que expressa o número de elementos de um sistema reduzido de resíduos mod n.

Definição 1.2.13 (Função ϕ de Euler). *Seja* $n \geq 1$. *O número de inteiros positivos menores ou iguais a* n *que são primos com* n *é denotado por* $\phi(n)$. *Esta função de* n *é chamada* função ϕ de Euler *ou, também, por* número indicador de Euler. *Simbolicamente, tem-se:*

$$\phi(n) = \sharp\{m \in \mathbb{N} : m \leq n \ \wedge \ (m,n) = 1\}.$$

Algumas propriedades básicas deste conceito:

- Se $a \equiv b \mod n$ e a é primo com n então também b é primo com n.
- Se p é primo então qualquer inteiro positivo menor que p é primo com p, portanto, $\phi(p) = p - 1$.

Lema 1.2.14 *Suponhamos que* $(a,n) = 1$. *Se* $a_1, a_2, \ldots, a_n$ *forma um sistema completo de resíduos. Então* $aa_1, aa_2, \ldots, aa_n$ *também forma um sistema completo de resíduos. Se* $a_1, a_2, \ldots, a_{\phi(n)}$ *forma um sistema reduzido de resíduos, então* $aa_1, aa_2, \ldots, aa_{\phi(n)}$ *também forma um sistema reduzido de resíduos.*

Demonstração: Vamos começar por provar a primeira parte. Como $(a,n) = 1$, então $aa_i \equiv aa_j \mod n$ implica $a_i \equiv a_j \mod n$, mas por definição de sistema completo de resíduos, isto não pode acontecer. Assim, $aa_i \not\equiv aa_j \mod n$ para $i \neq j$. O facto de a ser primo com n também implica que existe c tal que

$$ac \equiv 1 \mod n.$$

Seja d um inteiro. Então $cd \equiv a_i \mod n$, para algum $1 \leq i \leq n$. Donde,

$$d \equiv acd \equiv aa_i \mod n.$$

Portanto, $aa_1, aa_2, \ldots, aa_n$ também forma um sistema completo de resíduos.

Agora, se $(a, n) = 1$ e $(a_i, n) = 1$ então $(aa_i, n) = 1$. Portanto, os inteiros $aa_1, aa_2, \ldots, aa_{\phi(n)}$ também formam um sistema reduzido de resíduos. □

Este último resultado tem as seguintes consequências:

Teorema 1.2.15 (Teorema de Euler). *Se* $(a, n) = 1$ *então*

$$a^{\phi(n)} \equiv 1 \mod n.$$

Demonstração: Seja $a_1, a_2, \ldots, a_{\phi(n)}$ um sistema reduzido de resíduos. Pelo lema anterior, $aa_1, aa_2, \ldots, aa_{\phi(n)}$ também forma um sistema reduzido de resíduos. Mais, para cada $1 \leq i \leq \phi(n)$, $aa_i \equiv a_j \mod n$, para algum $1 \leq j \leq n$. Portanto,

$$aa_1 aa_2 \cdots aa_{\phi(n)} \equiv a_1 a_2 \cdots a_{\phi(n)} \mod n.$$

Como $(a_1 a_2 \cdots a_{\phi(n)}, n) = 1$ então, pelo teorema 1.2.9

$$a^{\phi(n)} \equiv 1 \mod n.$$

□

Teorema 1.2.16 (Pequeno Teorema de Fermat). *Se* p *é primo então*

$$a^p \equiv a \mod p,$$

para qualquer inteiro a.

Demonstração: Se $p \mid a$ então $a^p \equiv 0 \mod p$ e $a \equiv 0 \mod p$. Logo, $a^p \equiv a \mod p$. Se $p \nmid a$ então $(a, p) = 1$, e, pelo teorema de Euler, $a^{\phi(p)} \equiv 1 \mod p$. Mas $\phi(p) = p - 1$. Portanto, $a^p \equiv a \mod p$. □

Importa salientar que o teorema de Euler, em 1760, visou generalizar o pequeno teorema de Fermat, enunciado em 1640, para quaisquer números inteiros, utilizando, para isso, a função de Euler. É interessante notar, ainda, que para um número primo, o teorema de Euler é exatamente o pequeno teorema de Fermat.

De seguida iremos apresentar uma fórmula para $\phi(n)$ que depende da factorização em primos de n. Mas, antes precisamos de definir função multiplicativa.

Definição 1.2.17 (Multiplicativa). *Se a função $f(n)$ está definida para todos os inteiros positivos, então dizemos que $f(n)$ é* multiplicativa *se para qualquer par de inteiros positivos m e n, tais que $(m,n)=1$, se tem*

$$f(mn) = f(m)f(n).$$

Temos o seguinte resultado:

Teorema 1.2.18 *A função $\phi(n)$ é multiplicativa.*

Demonstração: Sejam m e n inteiros positivos tais que $(m,n)=1$. Vamos colocar os primeiros mn inteiros numa tabela com m colunas e n linhas, da seguinte forma:

1	2	...	m
m+1	m+2	...	m+m
2m+1	2m+2	...	2m+m
⋮	⋮	⋮	⋮
(n-1)m+1	(n-1)m+2	...	(n-1)m+m

Os números na coluna j são $0\cdot m+j$, $1\cdot m+j$, $2\cdot m+j,\ldots,(n-1)\cdot m+j$.

Mostremos, agora que, $(ma+j,m)=(j,m)$, para qualquer inteiro a. Consideremos $(j,m)=q$ e seja $r=(ma+j,m)$. Como $r|m$ então temos que $r|ma$ e tem-se também que $r|(ma+j)$, logo $r|(ma+j-ma)=j$. Assim, como $r|m$ e $r|j$ então $r|q$. Claramente, $q|(ma+j)$ e $q|m$ donde $q|r$ e, deste modo, temos $r=q$.

Portanto, ou qualquer elemento da coluna j é primo com m ou nenhum elemento da coluna j é primo com m. Assim, há exactamente $\phi(m)$ colunas contendo inteiros primos com m e qualquer elemento destas $\phi(m)$ colunas é primo com m.

Como $(m,n)=1$, os n elementos de cada coluna j formam um sistema completo de resíduos $\bmod n$. Portanto, por definição, cada coluna j contém exactamente $\phi(n)$ elementos primos com n. Donde, em cada uma das $\phi(m)$ colunas que têm os elementos que são primos com m, há exactamente $\phi(n)$ elementos primos com n. Mais, estes são os únicos elementos que são ao mesmo tempo primos com m e primos com n. Isto é, há exactamente $\phi(m)\phi(n)$ elementos na tabela que são primos com m e, ao mesmo tempo, primos com n.

Mas um inteiro é primo com mn se e só se for primo simultaneamente com m e com n. Portanto,

$$\phi(mn) = \phi(m)\phi(n)$$

e a função de Euler é multiplicativa. □

Teorema 1.2.19 *Suponhamos que a factorização de n em primos é a seguinte*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}.$$

Então

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Demonstração: Vamos começar por calcular $\phi(p^a)$, para p primo e $a \geq 1$. Um inteiro é primo com p^a excepto se for divisível por p. Os números de 1 a p^a que são divisíveis por p, são $1 \cdot p$, $2 \cdot p$, $\ldots$, $p^{a-1}p$. Portanto,

$$\phi(p^a) = p^a - p^{a-1} = p^a\left(1 - \frac{1}{p}\right).$$

Como a função $\phi(n)$ é multiplicativa, temos

$$\begin{aligned}
\phi(n) &= \phi(p_1^{a_1})\phi(p_2^{a_2})\cdots\phi(p_k^{a_k}) \\
&= p_1^{a_1}\left(1 - \frac{1}{p_1}\right) p_2^{a_2}\left(1 - \frac{1}{p_2}\right)\cdots p_k^{a_k}\left(1 - \frac{1}{p_k}\right) \\
&= p_1^{a_1} p_2^{a_2}\cdots p_k^{a_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).
\end{aligned}$$

□

Apresentamos mais um resultado auxiliar cuja demonstração pode ser consultada em [1].

Teorema 1.2.20 *Seja n um inteiro positivo. Então*

$$n = \sum_{d|n} \phi(d).$$

De seguida apresentamos como encontrar a menor potência positiva, r, tal que $a^r \equiv 1 \mod n$, assim como, os valores de a para os quais essa menor potência é $\phi(n)$.

Definição 1.2.21 (Ordem de a módulo n). *Suponhamos que $(a, n) = 1$. Definimos a* ordem *de a módulo n como sendo o menor inteiro positivo, digamos b, para o qual*

$$a^b \equiv 1 \mod n$$

e denotamo-lo por $ord_n(a)$.

Exemplo 1.2.22 : *$ord_7(10) = 6$, pois*

$$10^1 \equiv 3 \mod 7 \qquad 10^2 \equiv 2 \mod 7 \qquad 10^3 \equiv 6 \mod 7$$
$$10^4 \equiv 4 \mod 7 \qquad 10^5 \equiv 5 \mod 7 \qquad 10^6 \equiv 1 \mod 7$$

Pelo teorema de Euler, $\mathrm{ord}_n(a)$ existe sempre que $(a, n) = 1$, e

$$\mathrm{ord}_n(a) \leq \phi(n).$$

Vamos mostrar que a ordem de a módulo n divide $\phi(n)$.

Teorema 1.2.23 *Se $(a, n) = 1$ e se $a^b \equiv 1 \mod n$, para algum $b > 0$, então $ord_n(a) \mid b$. Em particular,*

$$ord_n(a) \mid \phi(n).$$

Reciprocamente, se $ord_n(a) \mid b$ então $a^b \equiv 1 \mod n$.

Demonstração: Seja $b > 0$ tal que $a^b \equiv 1 \mod n$ e $d = (\mathrm{ord}_n(a), b)$. Então $d \leq \mathrm{ord}_n(a)$. Temos $d = ub + v\mathrm{ord}_n(a)$, para alguns u e v inteiros, logo,

$$a^d \equiv \left(a^{ub+v\ \mathrm{ord}_n(a)}\right) \equiv \left(a^b\right)^u \times \left(a^{\mathrm{ord}_n(a)}\right)^v \equiv 1 \times 1 \equiv 1 \mod n.$$

Portanto, $a^d \equiv 1 \mod n$, donde $\text{ord}_n(a) \leq d$ (por definição de $\text{ord}_n(a)$). Logo

$$\text{ord}_n(a) = d.$$

Portanto, $\text{ord}_n(a) \mid b$.

Reciprocamente, se $\text{ord}_n(a) \mid b$, então $b = k\,\text{ord}_n(a)$, para algum inteiro k, e

$$a^b \equiv \left(a^{\text{ord}_n(a)}\right)^k \equiv 1 \mod n.$$

□

Definição 1.2.24 (Raiz primitiva). *Se $(a, n) = 1$ e $ord_n(a) = \phi(n)$, dizemos que a é uma* raiz primitiva *de n.*

Exemplo 1.2.25 *Consideremos $n = 10$. Há exatamente 4 inteiros em $\{1, 2, \ldots, 10\}$ que são primos com 10, logo $\phi(10) = 4$. Uma vez que $(3, 10) = 1$, $3^1 \equiv 3 \mod 10$, $3^2 \equiv 9 \mod 10$, $3^3 \equiv 7 \mod 10$ e $3^4 \equiv 1 \mod 10$, conclui-se que 3 é uma raíz primitiva módulo 10.*

O próximo resultado, cuja demonstração pode ser encontrada em [1], será usado na demonstração do teorema seguinte.

Teorema 1.2.26 *Se p é primo e $d \mid (p-1)$ então a congruência*

$$x^d \equiv 1 \mod p$$

tem exactamente d soluções distintas $\mod p$.

Teorema 1.2.27 *Seja p um primo e e d um inteiro tal que $d \mid (p-1)$. Então há exatamente $\phi(d)$ inteiros distintos $\mod p$ cuja ordem $\mod p$ é d. Em particular, há exatamente $\phi(p-1)$ raízes primitivas de p.*

Demonstração: Seja p um primo e seja $d \mid (p-1)$. Vamos provar por indução que há exatamente $\phi(d)$ elementos cuja ordem $\mod p$ é d. Efetivamente, 1 é o único elemento cuja ordem é 1. Seja $n > 1$ tal que $n \mid (p-1)$ e suponhamos que para qualquer $d < n$ tal

que $d \mid (p-1)$, há exatamente $\phi(d)$ elementos cuja ordem $\mod p$ é d. Consideremos a congruência

$$x^n \equiv 1 \mod p.$$

Pelo teorema 1.2.26, esta congruência tem exatamente n soluções. Se $d \mid n$ e $\mathrm{ord}_p(a) = d$ então a é solução da congruência. Mas, por indução, há exatamente $\phi(d)$ elementos com ordem d, para $d < n$. Como alude o teorema 1.2.20,

$$n = \sum_{d|n} \phi(d)$$

então temos exatamente $\phi(n)$ elementos cuja ordem $\mod p$ é n. Portanto, o teorema é válido para qualquer $n \mid (p-1)$. □

Capítulo 2

A mais-valia das dízimas

Vamos mostrar neste capítulo a riqueza adicional das dízimas, descobrindo resultados e inter-relações numéricas interessantes, tais como: o comprimento do período de uma dízima na base decimal, particularizando para uma dízima de uma fração cujo denominador é primo e, também, o comprimento do período em bases numéricas distintas; o fascinante teorema de Midy e a sua generalização; e, ainda, alguns critérios de divisibilidade por números primos associados à representação de números.

2.1 Representação de números por dízimas

Designamos por $[\alpha]$ a característica de um número real α, isto é, o maior número inteiro que é menor ou igual a α. Dado um número real positivo α, escrito da seguinte forma

$$\alpha = [\alpha] + x, \quad \text{com} \;\; 0 \leq x < 1.$$

Supondo que $[\alpha] > 0$, existirá um inteiro não negativo n tal que

$$10^n \leq [\alpha] < 10^{n+1}$$

e então, dividindo por 10^n, tem-se que

$$[\alpha] = A_1 10^n + X_1, \quad \text{com} \;\; 0 < A_1 = [10^{-n}\alpha] < 10, \;\; 0 \leq X_1 < 10^n.$$

Assim, por aplicação sucessiva do algoritmo da divisão, vamos obter:

$$X_1 = A_2 10^{n-1} + X_2, \;\; 0 \leq A_2 < 10, \;\; 0 \leq X_2 < 10^{n-1}$$

$$X_2 = A_3 10^{n-2} + X_3, \;\; 0 \leq A_3 < 10, \;\; 0 \leq X_3 < 10^{n-2}$$

$$\vdots$$

$$X_{n-1} = A_n 10 + X_n, \quad 0 \leq A_n < 10, \quad 0 \leq X_n < 10$$

$$X_n = A_{n+1}, \quad 0 \leq A_{n+1} < 10.$$

Desta forma, tem-se a representação

$$[\alpha] = A_1 10^n + A_2 10^{n-1} + \cdots + A_n 10 + A_{n+1},$$

que abreviado fica,

$$[\alpha] = A_1 A_2 \ldots A_n A_{n+1}, \quad \text{com} \quad A_1 \neq 0 \ \text{ e } \ 0 \leq A_i < 10 \ \text{ para } \ 1 \leq i \leq n+1,$$

que designamos por representação normal de um número inteiro na base 10.

No que concerne à parte fracionária (ou decimal), x, o processo é semelhante ao anterior. Seja $x = f_1$ e $a_1 = [10 f_1]$; a_1 é um número inteiro não negativo inferior a 10, pelo que podemos escrever

$$10 f_1 = a_1 + f_2, \quad \text{sendo } \ 0 \leq f_2 < 1.$$

Repetindo o processo, temos:

$$a_2 = [10 f_2], \quad 10 f_2 = a_2 + f_3,$$

sendo $0 \leq f_3 < 1$ e a_2 é um número inteiro não negativo inferior a 10, e assim sucessivamente. Se representarmos por x_m a soma

$$x_m = \frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_m}{10^m},$$

podemos escrever

$$x = x_m + g_{m+1},$$

$$\text{com} \quad 0 \leq g_{m+1} = \frac{f_{m+1}}{10^m} < \frac{1}{10^m}. \tag{2.1}$$

E se os a_i a partir de uma certa ordem fossem todos 9?

Consideremos o seguinte,

$$\begin{aligned} g_{m+1} = \sum_{i=m+1}^{+\infty} \frac{9}{10^i} &= 9 \sum_{i=m+1}^{+\infty} 10^{-i} \\ &= 9 \sum_{i=0}^{+\infty} 10^{-(i+m+1)} \\ &= 9 \times 10^{-(m+1)} \sum_{i=0}^{+\infty} 10^{-i} \\ &= 9 \times 10^{-(m+1)} \frac{1}{1-\frac{1}{10}} \\ &= 9 \times 10^{-(m+1)} \times \frac{10}{9} \\ &= 10^{-m} = \frac{1}{10^m} \end{aligned}$$

pelo resultado apresentado em (2.1), verificamos que é impossível! Como se tem $0 \leq a_i \leq 9$ para todo o i e $\lim_{x \to +\infty} g_{m+1} = 0$, a série

$$\sum_{i=1}^{+\infty} \frac{a_i}{10^i}$$

converge para x. Escrevemos então $x = 0, a_1 a_2 \cdots$. Qualquer dízima deste género representa um número real entre 0 e 1.

Reunindo as expressões obtidas atrás para a parte inteira e também para a parte fracionária podemos concluir o seguinte resultado:

Teorema 2.1.1 *Qualquer número real positivo α pode ser escrito na forma de uma dízima*

$$A_1 A_2 \cdots A_{n+1}, a_1 a_2 \cdots$$

com $0 \leq A_i < 10$, para $1 \leq i \leq n+1$ e $0 \leq a_j < 10$, para todo o natural j. Além disso, existe uma infinidade de a_j diferente de 9.

Após este resultado, e para identificar e/ou classificar esta forma de escrita de um número real positivo, observemos as seguintes definições:

Definição 2.1.2 (Permutação cíclica). *Sejam k e $c_1, c_2, \ldots, c_k$ inteiros positivos e seja $P = (c_1, c_2, \ldots, c_k)$. Dizemos que P' é uma* permutação cíclica *de P se existir $1 < i \leq k$ tal que*

$$P' = (c_i, c_{i+1}, \ldots, c_k, c_1, \ldots, c_{i-1}).$$

Definição 2.1.3 (Dízima Periódica). *Uma dízima $0, a_1 a_2 \cdots$ com $a_i \in \{0, 1, \ldots, 9\}$, para $i \geq 1$, diz-se* periódica *se existirem inteiros positivos n_0, p e $b_1, \ldots, b_p$ tais que*

$$a_{n_0+i+kp} = b_i, \text{ para quaisquer } k \geq 0 \text{ e } 1 \leq i \leq p,$$

representando-se, $0, a_1 \cdots a_{n_0}(b_1 \cdots b_p)$.

Definição 2.1.4 (Período). *Se uma dízima $0, a_1 a_2 \cdots$ com $a_i \in \{0, 1, \ldots, 9\}$, para $i \geq 1$ é periódica e p é o menor inteiro para o qual se tem a sequência $(b_1 \cdots b_p)$ $(b_j \in \{0, 1, \ldots, 9\}; 1 \leq j \leq p)$, chama-se* período *da dízima a esta sequência ou a qualquer permutação cíclica desta sequência.*

Exemplo 2.1.5 *Atendendo às definições 2.1.3 e 2.1.4, os períodos da dízima de*

$$\frac{1}{7} = 0.(142857)$$

e da dízima de

$$\frac{5}{7} = 0.(714285)$$

podem ser vistos como o mesmo período, pois basta passar alguns algarismos para fora da parte que é repetida, ou seja,

$$\frac{5}{7} = 0.(714285) = 0.7(142857).$$

Assim, podemos dizer que $\frac{1}{7}$ e $\frac{5}{7}$ têm o mesmo período. Na verdade, se 7 não divide m, a dízima de $\frac{m}{7}$ pode sempre ser escrita de forma a obtermos o período (142857).

Definição 2.1.6 (Dízima puramente periódica; Anteperíodo; Comprimento do período e Dízima finita). *Se uma dízima $0, a_1 a_2 \cdots$ com $a_i \in \{0, 1, \ldots, 9\}$, para $i \geq 1$ é periódica de período $(b_1 \cdots b_p)$ e $n_0 = 0$ (ou seja, $a_1 = b_1$), diz-se que é* puramente periódica, *caso contrário é uma dízima mista e $a_1 \cdots a_{n_0}$ designa-se por* anteperíodo *e ao inteiro p chama-se* comprimento *do período. Uma dízima de período* (0) *diz-se* finita.

Em seguida, vamos estudar os números que podem ser representados por dízimas finitas ou infinitas periódicas que são os números racionais.

Apresentamos, de seguida, uma noção de número racional.

Definição 2.1.7 (Número racional). *Um número x diz-se um* número racional *se puder ser representado por $x = \frac{m}{q}$, onde m e q são números inteiros e $q \neq 0$.*

Definição 2.1.8 (Fração irredutível). *Se $m > 0$ e m e q são primos entre si, $\frac{m}{q}$ diz-se uma* fração irredutível.

Exemplo 2.1.9 : $\frac{310}{44} = \frac{155}{22} = 7 + \frac{1}{22}$.

Observação 2.1.10 *Seja $x = \frac{m}{q}$ um número racional. Tomando $d = (m, q)$, $m = dm_1$ e $q = dq_1$ então temos $x = \frac{m_1}{q_1}$. Se $d = (m, q)$ então $\left(\frac{m}{d}, \frac{q}{d}\right) = 1$, logo $(m_1, q_1) = 1$. Então qualquer número racional pode ser representado por uma fração irredutível.*

No desenvolvimento deste texto daremos primazia aos números racionais positivos, pelo que apresentamos o seguinte resultado:

Teorema 2.1.11 *Seja x um número real positivo. O número x é um número racional se e só se tem uma dízima periódica.*

Demonstração: Para verificarmos este resultado vamos mostrar, em primeiro lugar, que se x tem uma dízima periódica então é racional.

Se x é um número real então $x = [x] + x_1$, onde $x_1 = 0, a_1 a_2 \cdots$ com $a_i \in \{0, 1, \ldots, 9\}$.

Suponhamos que x tem uma dízima periódica então

$$x_1 = 0, a_1 \cdots a_{n_0}(b_1 \cdots b_p),$$

com p inteiro positivo, $b_j \in \{0, 1, \ldots, 9\}$, para $1 \leq j \leq p$.

Assim,

$$\begin{aligned} x_1 &= \sum_{i=1}^{n_0} a_i 10^{-i} + \sum_{s=0}^{\infty}\sum_{i=1}^{p} b_i 10^{-(n_0+sp+i)} \\ &= \frac{1}{10^{n_0}} \sum_{i=1}^{n_0} 10^{n_0-i} a_i + \sum_{i=1}^{p} b_i 10^{-(n_0+i)} \sum_{s=0}^{\infty} 10^{-sp} \\ &= \frac{1}{10^{n_0}} \sum_{i=1}^{n_0} a_i 10^{n_0-i} + \frac{1}{10^{n_0+p}} \left(\sum_{i=1}^{p} b_i 10^{p-i} \right) \times \frac{10^p}{10^p - 1}. \end{aligned}$$

Como todas as somas na última expressão são finitas temos que o número x_1 é racional.

Resta-nos mostrar que se x é um número racional então tem uma dízima periódica.

Se x é racional, como $x = [x] + x_1$ então podemos escrever $x_1 = \dfrac{m}{q}$ com m e q inteiros positivos, $(m, q) = 1$ e $m < q$.

Podemos também escrever $q = 2^a 5^b n$, com a e b inteiros não negativos e n um inteiro maior ou igual a 1, tal que $(n, 10) = 1$.

Seja $\mu = max\{a, b\}$. Se $n = 1$, temos

$$\begin{aligned} x_1 &= \frac{10^\mu m}{10^\mu 2^a 5^b} \\ &= \frac{2^{\mu-a} 5^{\mu-b} m}{10^\mu}, \end{aligned}$$

isto é,

$$10^\mu x_1 = 2^{\mu-a} 5^{\mu-b} m.$$

Vimos anteriormente, que $x_1 = 0, a_1 a_2 \cdots$, logo temos $a_j = 0$ para qualquer $j \geq \mu+1$, ou seja, x_1 tem uma dízima periódica com período (0) (x_1 tem uma dízima finita).

Se $n > 1$ temos,

$$\begin{aligned} a_1 a_2 \cdots a_\mu a_{\mu+1} a_{\mu+2} \cdots &= 10^\mu x_1 \\ &= \frac{2^{\mu-a} 5^{\mu-b} m}{n} \\ &= \frac{m_1}{n}, \end{aligned}$$

para algum m_1 inteiro positivo.

Como $(m, q) = 1$ e $(n, 10) = 1$ então $(m_1, n) = 1$ e, pelo algoritmo da divisão, podemos escrever $m_1 = q_0 n + r_0$, onde $q_0 = [10^\mu x_1] = a_1 \cdots a_\mu$ e $r_0 < n$. Temos também $(r_0, n) = 1$, pois $(m_1, n) = 1$.

Definindo recursivamente r_i, com $i \geq 1$, por

$$10r_{i-1} = a_{\mu+i} + r_i,$$

temos $1 \leq r_i < n$ e $(r_i, n) = 1$. Como há somente um número finito de valores que os r_i's podem tomar, vamos ter $r_j = r_{j+k}$, para algum $j \geq 0$ e algum $k \geq 1$.

Portanto,

$$\begin{aligned} 10r_j &= a_{\mu+j+1}n + r_{j+1} \\ &= a_{\mu+j+k+1}n + r_{j+1}, \end{aligned}$$

isto é,

$$a_{\mu+j+i} = a_{\mu+j+sk+i},$$

para quaisquer inteiros $1 \leq i \leq k-1$ e $s \geq 1$, ou seja, x_1 tem uma dízima periódica, portanto, x também tem uma dízima periódica. □

Observação 2.1.12 *Na próxima secção veremos que r tem uma dízima infinita puramente periódica.*

2.2 Comprimento do período de uma dízima

Tendo já presente a noção de período, apresentamos, agora, como determinar o comprimento do período de uma dízima periódica.

Vejamos o seguinte resultado.

Teorema 2.2.1 *Seja $x = \frac{p}{q}$ uma fração irredutível (p e $q \in \mathbb{N}$). Então:*

(1) *a dízima de x é finita se e só se q não admite outros factores primos para além de 2 e 5; mais precisamente, se $q = 2^\alpha 5^\beta$, então a dízima termina após μ algarismos, sendo $\mu = max(\alpha, \beta)$;*

(2) *se $(q, 10) = 1$, a dízima de x é infinita periódica pura com comprimento do período λ, sendo λ a ordem de 10 módulo q;*

(3) *se $q = 2^\alpha 5^\beta n$, sendo n um número natural maior que 1 e primo com 10, a dízima é periódica mista, com um período de comprimento λ (a ordem de 10 módulo n) e um anteperíodo de μ algarismos ($\mu = max(\alpha, \beta)$).*

Demonstração:

(1) Suponhamos então que $x = \frac{p}{q}$. A correspondente dízima termina se e só se existir um número natural i tal que $10^i x$ seja um número inteiro. Então, se $q = 2^\alpha 5^\beta$, basta considerar $i = max(\alpha, \beta)$ para se obter o resultado. Reciprocamente, se na decomposição de q em factores surgir um primo p_1 distinto de 2 e 5, a dízima não pode ser finita. Pois, se existisse um natural i tal que $10^i \frac{p}{q} = k$ é inteiro, ficaria $10^i p = k \times q$ e p_1 dividiria o segundo membro e não o primeiro (pois supomos que $(p, q) = 1$), o que é absurdo.

Relativamente ao comprimento da dízima, consideremos o seguinte:

seja $x = \frac{p}{q}$ em que $q = 2^\alpha 5^\beta$, com α e $\beta \geq 0$ e $\mu = max\{\alpha, \beta\}$, procedendo da seguinte forma, temos:

$$x = \frac{p2^{\mu-\alpha}5^{\mu-\beta}}{2^\alpha 5^\beta 2^{\mu-\alpha}5^{\mu-\beta}} = \frac{p2^{\mu-\alpha}5^{\mu-\beta}}{10^\mu}$$

e, claramente, temos uma potência de 10 no denominador.

Assim, concluímos, que o comprimento da dízima é igual a α ou β, ou seja tem μ algarismos, com $\mu = max(\alpha, \beta)$.

(2) Suponhamos agora que $(q, 10) = 1$. Seja λ a ordem de 10 módulo q (cuja existência é garantida pelo teorema de Euler).

Considerando novamente $x = \frac{p}{q}$, temos para algum inteiro m, $10^\lambda = mq + 1$ e então, para certos k, $r \in \mathbb{N}_0$, com $0 < r < 10^\lambda - 1$,

$$\begin{aligned} 10^\lambda x = 10^\lambda \frac{p}{q} &= \frac{(mq+1)p}{q} = mp + \frac{p}{q} = mp + x, \text{ donde} \\ x &= \frac{mp}{10^\lambda - 1} = k + \frac{r}{10^\lambda - 1} \\ &= k + \frac{r}{10^\lambda} \frac{1}{1 - \frac{1}{10^\lambda}}. \end{aligned}$$

Tomando $r = \sum_{i=1}^{\lambda} 10^{\lambda-i} a_i$, para certos $a_i \in \mathbb{N}_0$, temos o seguinte:

$$\begin{aligned} x &= k + \left(\sum_{i=1}^{\lambda} \frac{a_i}{10^i} \right) \sum_{n=0}^{\infty} \frac{1}{10^{n\lambda}} \\ &= k + 0, (a_1 \cdots a_\lambda). \end{aligned}$$

Portanto, a dízima de x é puramente periódica, com período de comprimento λ.

Por outro lado, dada uma dízima infinita periódica pura de período $(a_1 \cdots a_k)$ temos que

$$\begin{aligned} 0,(a_1 \cdots a_k) &= \left(\frac{a_1}{10} + \cdots + \frac{a_k}{10^k}\right)\left(1 + \frac{1}{10^k} + \frac{1}{10^{2k}} + \cdots\right) \\ &= \frac{a_1 10^{k-1} + a_2 10^{k-2} + \cdots + a_k}{10^k - 1} = \frac{p}{q} \end{aligned}$$

para certos números naturais p e q, primos entre si. Então

$$q(a_1 10^{k-1} + a_2 10^{k-2} + \cdots + a_k) = p(10^k - 1),$$

logo q divide $p(10^k - 1)$ e $(p, q) = 1$, então deduz-se que q divide $10^k - 1$, ou seja, $10^k \equiv 1 \mod q$, pelo que $k \geq \lambda$. Atendendo à definição 2.1.4, segue-se que $k = \lambda$. Portanto, a dízima é periódica com comprimento igual à ordem de 10 módulo q.

(3) Suponhamos agora que $x = \frac{p}{q}$, com $q = 2^\alpha 5^\beta n$, sendo n um número natural maior que 1 e primo com 10. Seja λ a ordem de 10 módulo n e $\mu = max(\alpha, \beta)$, então

$$10^\mu x = \frac{10^\mu p}{2^\alpha 5^\beta n} = X + \frac{p_1}{n}$$

com X inteiro não negativo, $0 < p_1 < n$ e $(p_1, n) = 1$. Supondo que $X > 0$, X pode representar-se na base 10, ou seja, $X = A_1 A_2 \cdots A_m$, pois atendendo ao ponto (2) anterior, a fração $\frac{p_1}{n}$ é periódica de período λ e podemos escrever

$$10^\lambda x = A_1 A_2 \cdots A_m, (b_1 \ldots b_\lambda)$$

ou seja, $x = A_1 A_2 \cdots A_{m-\mu}, a_1 a_2 \cdots a_\mu, (b_1 \cdots b_p)$, onde $a_i = A_{m-\mu+i}$.

E, assim, concluímos a demonstração do teorema.

□

Exemplo 2.2.2 : *Para exemplificar o caso (2), consideremos* $x = \frac{3}{37}$. *Temos* $(37, 10) = 1$ *e como* $ord_{37}(10) = 3$, *o comprimento do período é* 3. *Então,*

$$10^3 x = \frac{(27 \times 37 + 1) \times 3}{37} = 27 \times 3 + \frac{3}{37} = 27 \times 3 + x,$$

donde $x = \frac{81}{1000} \times \sum_{n=0}^{\infty} \frac{1}{1000^n} = 0,(081)$.

Exemplo 2.2.3 : *Para exemplificar o caso (3), consideremos* $x = \frac{3}{140}$. *Como* $140 = 2^2 \times 5 \times 7$, *temos* $\alpha = 2$, $\beta = 1$ *e* $n = 7$, *logo* $\mu = 2$. *Então,* $10^2 x = \frac{15}{7} = 2 + \frac{1}{7} = 2,(142857)$ *e dividindo tudo por* 100, *obtemos* $\frac{3}{140} = 0,02(142857)$.

2.2.1 Comprimento do período para um denominador primo

Para uma dízima de uma fração cujo denominador é 3, existem dois períodos distintos, (3) e (6),

$$\frac{1}{3} = 0,333\ldots, \quad \frac{2}{3} = 0,666\ldots,$$

assim como, existem cinco períodos distintos, (09), (18), (27), (36), (45), para uma dízima de uma fração com denominador 11,

$$\frac{1}{11} = 0,090909\ldots, \quad \frac{2}{11} = 0,181818\ldots, \quad \frac{3}{11} = 0,272727\ldots,$$

$$\frac{4}{11} = 0,363636\ldots, \quad \frac{5}{11} = 0,454545\ldots,$$

enquanto para

$$\frac{10}{11}, \quad \frac{9}{11}, \quad \frac{8}{11}, \quad \frac{7}{11}, \quad \frac{6}{11}$$

os respetivos períodos são os mesmos em relação aos períodos anteriores apenas com alterações de posições dos algarismos, ou seja,

$$\frac{10}{11} = 0,909090\ldots, \quad \frac{9}{11} = 0,818181\ldots, \quad \frac{8}{11} = 0,727272\ldots,$$

$$\frac{7}{11} = 0,636363\ldots, \quad \frac{6}{11} = 0,545454\ldots.$$

Vejamos para uma dízima de uma fração com denominador 13 onde existem dois períodos distintos com comprimento 6, devido ao facto das potências de 10 mod 13 se repetirem de 6 em 6:

$$10^0 \equiv 1; \;\; 10^1 \equiv 10; \;\; 10^2 \equiv 9; \;\; 10^3 \equiv 12; \;\; 10^4 \equiv 3; \;\; 10^5 \equiv 4; \;\; 10^6 \equiv 1.$$

Portanto, o primeiro período (076923) da dízima de $\frac{1}{13} = 0,076923\ldots$ em que os períodos das dízimas das frações $\frac{3}{13}$, $\frac{4}{13}$, $\frac{9}{13}$, $\frac{10}{13}$ e $\frac{12}{13}$ são respetivas permutações cíclicas, enquanto os períodos das dízimas das frações $\frac{5}{13}$, $\frac{6}{13}$, $\frac{7}{13}$, $\frac{8}{13}$ e $\frac{11}{13}$ são respetivas permutações cíclicas do período (153846) da dízima de $\frac{2}{13} = 0,153846\ldots$.

Perante o exposto, podemos observar o seguinte:

Dado um inteiro positivo q primo (diferente de 2 e 5), há um conjunto $\mathcal{P}$ de períodos, tal que qualquer dízima de uma fração que tenha q como denominador vai ter uma sequência pertencente a $\mathcal{P}$ ou a uma permutação cíclica dessa sequência pertencente a $\mathcal{P}$.

Perante esta observação, podemos apresentar dois resultados:

Teorema 2.2.4 *Dado um primo q diferente de 2 e 5, os períodos das dízimas de fracções irredutíveis da forma $x = \frac{p}{q}$ têm todos o mesmo comprimento.*

Demonstração: Seja x uma fração irredutível da forma $\frac{p}{q}$, q primo e $(10, q) = 1$ e um inteiro não negativo $p \in \{1, 2, \ldots, q-1\}$. Claramente, q não divide p.

Pelo ponto (2) do teorema 2.2.1, $x = \frac{p}{q}$ é do tipo $x = k + 0,(a_1 \ldots a_\lambda)$, onde λ é a ordem de 10 módulo q. Deste modo, x tem uma dízima infinita periódica cujo período tem comprimento λ, qualquer que seja p. □

Em relação ao número de períodos diferentes de uma fração cujo denominador é primo diferente de 2 e 5, apresentamos o seguinte resultado:

Teorema 2.2.5 *Seja q um primo, com $(q, 10) = 1$. Sejam $x_1 = \frac{1}{q}, \ldots, x_{q-1} = \frac{q-1}{q}$ os números racionais menores que 1 que podem ser representados por frações irredutíveis cujo denominador é q. Então o número de períodos diferentes que as dízimas de $x_1, \ldots, x_{q-1}$ podem ter é igual a $\frac{q-1}{\lambda}$ onde λ é a ordem de 10 módulo q.*

Demonstração: Seja q primo e $\lambda = \mathrm{ord}_q(10)$ o comprimento do período da dízima de uma fração $\frac{p}{q}$. Atendendo ao teorema 1.2.23, λ divide $q-1$. Pretendemos demonstrar que o número de períodos diferentes é exatamente $\frac{q-1}{\lambda}$, onde q é um denominador primo.

Pelo teorema 2.2.4, todas as frações irredutíveis com o mesmo denominador têm dízimas cujos períodos têm o mesmo comprimento. Considerando $1 \leq p \leq q-1$ há ao todo, essencialmente, $q-1$ frações diferentes. Portanto, existem λ frações para cada período, uma vez que temos λ permutações cícilicas do período. Assim, vamos ter, exatamente, $\dfrac{q-1}{\lambda}$ períodos diferentes. □

Da tabela seguinte, claramente, verificamos que tanto o n - número de períodos diferentes - como o λ - comprimento dos períodos - dividem, exatamente, $q-1$.

$\boldsymbol{q}$	3	7	11	13	17	19	23	29	31	37	41	43	47	53	59
$\boldsymbol{n}$	2	1	5	2	1	1	1	1	2	12	8	2	1	4	1
λ	1	6	2	6	16	18	22	28	15	3	5	21	46	13	58
$\boldsymbol{q}$	61	67	71	73	79	83	89	97	101	103	107	109	113	127	131
$\boldsymbol{n}$	1	2	2	9	6	2	2	1	25	3	3	1	1	3	1
λ	60	33	35	8	13	41	44	96	4	34	53	108	112	42	130
$\boldsymbol{q}$	137	139	149	151	157	163	167	173	179	181	191	193	197	199	211
$\boldsymbol{n}$	17	3	1	2	2	2	1	2	1	1	2	1	2	2	7
λ	8	46	148	75	78	81	166	86	178	180	95	192	98	99	30
$\boldsymbol{q}$	223	227	229	233	239	241	251	257	263	269	271	277	281	283	293
$\boldsymbol{n}$	1	2	1	1	34	8	5	1	1	1	54	4	10	2	1
λ	222	113	228	232	7	30	50	256	262	268	5	69	28	141	146

Tabela 2.1: Para denominador primo $\boldsymbol{q}$ (diferente de 2 e 5), $\boldsymbol{n}$ - número de períodos diferentes e λ - comprimento do período, (base 10)

Da observação da tabela, verificamos que existem números primos, como: 7, 17, 19, 23, 29, 47, 59, 61, 97, 109, 113, 131, 149, 167, ... cujo comprimento do seu período, na base 10, é igual a: 6, 16, 18, 22, 29, 46, 58, 60, 96, 108, 112, 130, 148, 166, ...

Esta observação motiva a seguinte definição, para uma qualquer base numérica b ($b > 1$):

Definição 2.2.6 (Número primo longo). *Seja q um primo. Dizemos que q é um* número primo longo *na base b ($b > 1$) se a dízima de $\dfrac{1}{q}$ não é finita e o comprimento do seu período é $q-1$.*

Recorrendo ao resultado vertido no teorema 1.2.23, concluímos o seguinte:

Observação 2.2.7 *Para um denominador q primo longo em b ($b > 1$) a ordem de 10 módulo q é $q-1$. Se $n = \dfrac{q-1}{ord_q 10}$ é o número de períodos diferentes então n é igual a 1.*

Portanto, todas as dízimas infinitas periódicas de $\frac{1}{q}, \frac{2}{q}, \ldots, \frac{q-1}{q}$ *têm o mesmo período, cujos algarismos são permutações cíclicas dos algarismos do período de* $\frac{1}{q}$.

Estima-se que cerca de 37% dos números primos sejam longos, na base 10. Em 1927, Emil Artin [13] conjeturou para este número a expressão,

$$\frac{1}{2} \times \frac{5}{6} \times \frac{19}{20} \times \frac{41}{42} \times \frac{109}{110} \times \frac{155}{156} \times \cdots = 0,3739558136 \cdots = C$$

de outra forma,

$$C = \prod_{q} \left(1 - \frac{1}{q(q-1)}\right) = \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3 \times 2}\right)\left(1 - \frac{1}{5 \times 4}\right)\left(1 - \frac{1}{7 \times 6}\right) \cdots$$

onde a cada número primo q corresponde um fator da expressão numérica anterior.

2.2.2 Comprimento do período em bases distintas

Apresentamos agora a representação de um número inteiro positivo α, num sistema de representação genérico de base b (sendo b um número natural maior que 1), da seguinte forma:

Definição 2.2.8 *Dados inteiros* $n > 0$ *e* $b > 1$, $d_1, \ldots, d_n \in \{0, 1, \ldots, b-1\}$, *representamos o inteiro*

$$\alpha = d_n + d_{n-1}b + \cdots + d_2 b^{n-2} + d_1 b^{n-1},$$

por $(d_1 d_2 \cdots d_{n-1} d_n)_b$.

Salientamos que se $b = 10$ escrevemos $d_1 d_2 \cdots d_{n-1} d_n$ em vez de $(d_1 d_2 \cdots d_{n-1} d_n)_{10}$.

Apresentamos, ainda, a seguinte definição necessária para o desenvolvimento de determinados conceitos que serão, posteriormente, introduzidos.

Definição 2.2.9 (Permutação cíclica de α). *Sejam* k, $b(>1)$ *e* $\alpha_b = (d_1 d_2 \cdots d_k)_b$ *inteiros positivos. Dizemos que* α' *é uma* permutação cíclica *de* α *se existir* $1 < i \leq k$ *tal que* $\alpha' = d_i d_{i+1} \cdots d_k d_1 \cdots d_{i-1}$.

Exemplo 2.2.10 :

(1) $\frac{2}{7} = \frac{0}{2} + \frac{1}{2^2} + \frac{0}{2^3} + \frac{0}{2^4} + \frac{1}{2^5} + \frac{0}{2^6} + \cdots = (0,(010))_2$

(2) $\frac{1}{3} = \frac{1}{5} + \frac{3}{5^2} + \frac{1}{5^3} + \frac{3}{5^4} + \cdots = (0,(13))_5$

(3) $\frac{2}{7} = \frac{2}{8} + \frac{2}{8^2} + \frac{2}{8^3} + \cdots = (0,(2))_8$

Perante os exemplos apresentados, uma interrogação se coloca: como se comporta o comprimento do período da dízima de uma fração, quando esta é representada em bases numéricas distintas? Comecemos por observar o caso da fração $\frac{1}{11}$ em várias bases:

- base 2: $\frac{1}{11} = 0,(0001011101)$ comprimento do período 10;
- base 3: $\frac{1}{11} = 0,(00211)$ comprimento do período 5;
- base 4: $\frac{1}{11} = 0,(01131)$ comprimento do período 5;
- base 5: $\frac{1}{11} = 0,(02114)$ comprimento do período 5;
- base 6: $\frac{1}{11} = 0,(0313452421)$ comprimento do período 10;
- base 7: $\frac{1}{11} = 0,(0431162355)$ comprimento do período 10;
- base 8: $\frac{1}{11} = 0,(0564272135)$ comprimento do período 10;
- base 9: $\frac{1}{11} = 0,(07324)$ comprimento do período 5;
- base 10: $\frac{1}{11} = 0,(09)$ comprimento do período 2;
- base 11: $\frac{1}{11} = 0,1$ dízima finita;
- base 12: $\frac{1}{11} = 0,(1)$ comprimento do período 1.

Facilmente verificamos que o comprimento do período é a ordem de b módulo 11, portanto, depende do valor de b módulo p, isto é, da base numérica b.

Resumindo, temos que o comprimento é igual a:

10	para 4 bases	b=2, 6, 7, 8 módulo 11
5	para 4 bases	b=3, 4, 5, 9 módulo 11
2	para 1 bases	b=10 módulo 11
1	para 1 bases	b=1 módulo 11

Podemos ainda estabelecer uma comparação entre os comprimentos dos períodos obtidos nas diferentes bases para a fração $\frac{1}{11}$ e o comportamento das frações $\frac{0}{10}, \frac{1}{10}, \ldots, \frac{8}{10}, \frac{9}{10}$.

Portanto, considerando as frações na forma irredutível, temos o menor denominador que é:

- 10 para 4 frações: $\frac{1}{10}, \frac{3}{10}, \frac{7}{10}, \frac{9}{10}$;
- 5 para 4 frações: $\frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}$;
- 2 para 1 fração: $\frac{1}{2}$;
- 1 para 1 fração: $\frac{0}{1}$.

Esta conclusão motiva o seguinte resultado geral:

- **Regra do indicador de Euler(ver[9, 26])**

  O número de bases, módulo p, nas quais $\frac{1}{p}$, tem períodos de comprimento λ é exatamente o mesmo que o número de frações

  $$\frac{0}{p-1}, \frac{1}{p-1}, \cdots, \frac{p-2}{p-1}$$

  que têm o menor denominador λ.

Utilizando um resultado apresentado no capítulo 1, o **número indicador de Euler**, $\phi(n)$, através da seguinte expressão:

$$\phi(n) = n \times \left(1 - \frac{1}{p_1}\right) \times \left(1 - \frac{1}{p_2}\right) \times \left(1 - \frac{1}{p_3}\right) \times \cdots \times \left(1 - \frac{1}{p_k}\right)$$

onde $p_1, p_2, p_3, \ldots, p_k$ são os diferentes divisores primos de n, podemos obter o seguinte:

$$\phi(10) = 4; \quad \phi(5) = 4; \quad \phi(2) = 1; \quad \phi(1) = 1.$$

Confrontando os comprimentos 10, 5, 2 e 1 dos períodos das dízimas, obtidos em diferentes bases, da dízima de $\frac{1}{11}$, com estes valores encontrados verificamos que também determinam o número de bases, $\mod 11$ que têm esses comprimentos.

Já vimos que 7 é um número primo longo na base 10. Sê-lo-á também, por exemplo, na base 2? Recorrendo ao **número indicador de Euler** obtemos $\phi(6) = 2$, ou seja, temos duas bases onde 7 é um número primo longo. Porém, como a ordem de 2 módulo 7 é igual a 3, tal como se verifica,

$$2^0 \equiv 1 \mod 7,\ 2^1 \equiv 2 \mod 7,\ 2^2 \equiv 4 \mod 7,\ 2^3 \equiv 1 \mod 7,$$

$$2^4 \equiv 2 \mod 7, \ldots.$$

concluímos que, não é longo na base 2! Procedendo desta forma, encontraremos que 7 é longo nas bases 10 e 3.

Constatámos ainda, pelo exemplo anterior, que o número primo 11 é longo na base 2, mas não na base 10. Recorrendo ao **número indicador de Euler** obtemos $\phi(10) = 4$, ou seja, temos quatro bases onde 11 é um número primo longo, como foi possível observar no exemplo atrás.

Tendo em conta, ainda, a **Regra do indicador de Euler** haverá sempre bases nas quais p é um número longo, uma vez que há certamente frações cujo menor denominador possível é $p-1$. Deste modo, concluímos o seguinte resultado:

Teorema 2.2.11 *Se p é número primo longo então há $\phi(p-1)$ bases, módulo p, isto é o mesmo que dizer que há $\phi(p-1)$ raízes primitivas de p, portanto, há $\phi(p-1)$ elementos cuja ordem é $p-1$.*

Este resultado resulta do teorema 1.2.27.

2.2.3 Aplicação: Baralhar cartas repetidamente

Se baralharmos as cartas de jogar repetidamente com o mesmo processo um certo número de vezes, as cartas voltam todas à posição inicial. Qual será esse número para a forma de baralhar em cascata interior?

Observemos a figura seguinte:

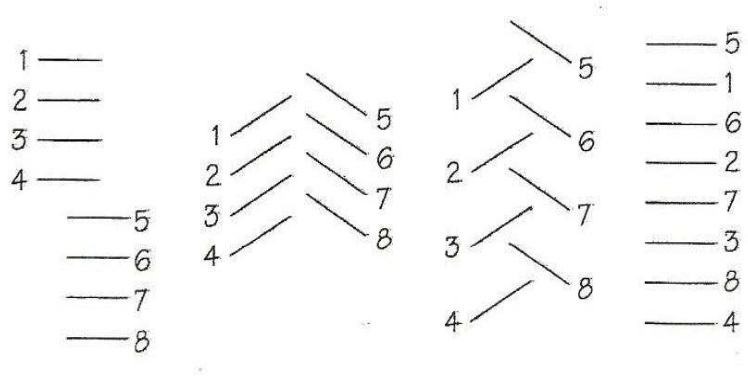

Figura 2.1: Baralhar em cascata interior

Consideremos um baralho de 52 cartas (em geral, $2n$ cartas), dividindo o baralho em duas partes iguais, ficamos com dois montes de 26 cartas cada (isto é, em geral n cartas). Se baralharmos então em cascata interior, começando primeiro pela mão direita, com a segunda parte ordenada do baralho, depois a mão esquerda, com a primeira parte ordenada do baralho, e assim sucessivamente, reparamos que logo após a primeira vez que realizamos este procedimento, a carta que estava na posição 1 está agora na posição 2, a carta que estava na posição 2 ocupa agora a posição 4, e assim por aí adiante. Deste modo, a carta passa para a posição $2i \mod 53$ (em geral, passa para a posição $2i \mod 2n+1$). Após baralharmos k vezes, a carta que no início estava na posição i, passa para a posição $2^k i \mod 53$ (em geral, passa para a posição $2^k i \mod 2n+1$). Portanto, as cartas só voltam à posição original quando baralharmos λ vezes, onde $\lambda = \text{ord}_{2n+1}2$. Como 2 é uma raíz primitiva de 53, no caso de utilizarmos as habituais 52 cartas, só voltamos ao início após baralharmos as cartas 52 vezes.

Nesta aplicação verificamos que há posições que se repetem após um determinado número de vezes, o que corresponde ao comportamento do período, na base 2, da dízima da fração $\frac{m}{53}$, com $m \neq 0$.

2.3 Teorema de Midy

Recordando a dízima de $\frac{1}{7} = 0,142857142857\ldots$, em que o conjunto de algarismos (142857) se repete, tratando-se, portanto, de uma dízima infinita periódica de período (142857) em que o seu comprimento é 6. Se dividirmos o conjunto de algarismos em dois números com o mesmo comprimento, obtemos: 142 e 857. Se os adicionarmos, temos $142 + 857 = 999$. Deste modo obtemos um número formado apenas com o algarismo

9. A analogia deste resultado mantém-se verdadeira, para todo o número da forma $\frac{p}{q}$, com q primo diferente de 2 e 5 e também p primo com q, se o comprimento do período da dízima de $\frac{p}{q}$ é um número par. Acabamos de apresentar o **Teorema de Midy**. Este resultado foi publicado em 1830 por um matemático francês E. Midy (ver [19]), mas ficou esquecido até ser redescoberto em 2004 por Brian Ginsberg (ver [12]), altura em que também foi generalizado.

Teorema 2.3.1 (Teorema de Midy). *Seja p um inteiro positivo, q primo $\neq 2$ e 5, p primo com q e $p < q$. Seja s a ordem de 10 módulo q e $s = 2s'$, com s' inteiro positivo, então tem-se que $\frac{p}{q} = 0,(u_1u_2)$ onde $u_1 = a_1a_2\cdots a_{s'}$ e $u_2 = a_{s'+1}a_{s'+2}\cdots a_{2s'}$, com $0 \leq a_i < 10$, (para qualquer $1 \leq i \leq 2s'$) e*

$$u_1 + u_2 = 10^{s'} - 1.$$

Demonstração: Suponhamos que $\frac{p}{q}$ tem um período de comprimento s igual a $2s'$ e, portanto, $\frac{p}{q} = 0,(u_1u_2)$. Multiplicando por $10^{s'}$ temos $10^{s'}\frac{p}{q} = u_1,(u_2u_1)$.

O denominador q não divide $10^{s'} - 1$ porque s é o menor inteiro positivo tal que $10^s \equiv 1 \mod q$, portanto q divide $10^s - 1$ e $s' < s$.

Sendo $10^{2s'} - 1 = (10^{s'} - 1)(10^{s'} + 1)$ e $(q, 10^{s'} - 1) = 1$ então pelo teorema 1.2.6 q divide $10^{s'} + 1$, donde $10^{s'} + 1 \equiv 0 \mod q$.

Adicionando,

$$\frac{p}{q} + 10^{s'}\frac{p}{q} = \frac{(10^{s'} + 1)p}{q},$$

utilizando o resultado anterior, que $10^{s'} + 1 \equiv 0 \mod q$, concluímos que é inteiro, isto é, que $0,(u_1u_2) + 0,(u_2u_1)$ é inteiro. Esta soma fica compreendida entre 0 e 2, exclusive.

Deste modo, temos $0,(u_1u_2) + 0,(u_2u_1) = 1$. Como,

$$0,(u_1u_2) = u_1(10^{-s'} + 10^{-3s'} + 10^{-5s'} + \cdots) + u_2(10^{-2s'} + 10^{-4s'} + 10^{-6s'} + \cdots)$$

$$0,(u_2u_1) = u_2(10^{-s'} + 10^{-3s'} + 10^{-5s'} + \cdots) + u_1(10^{-2s'} + 10^{-4s'} + 10^{-6s'} + \cdots),$$

logo,

$$0,(u_1u_2) + 0,(u_2u_1) = (u_1 + u_2) \times 10^{-s'} \times (1 + 10^{-s'} + 10^{-2s'} + 10^{-3s'} + \cdots) = 1.$$

Como, $1 + 10^{-s'} + 10^{-2s'} + 10^{-3s'} + \cdots = \dfrac{1 - \lim_{x\to+\infty} 10^{-is'}}{1 - 10^{-s'}} = \dfrac{1}{1 - 10^{-s'}}$, obtemos,

$$\frac{(u_1 + u_2)}{1 - 10^{-s'}} 10^{-s'} = 1,$$

o que, finalmente, fica:

$$u_1 + u_2 = \frac{1 - 10^{-s'}}{10^{-s'}} = 10^{s'} - 1.$$

□

Exemplo 2.3.2 :

(1) $\dfrac{1}{11} = 0,(09); \dfrac{2}{11} = 0,(18); \dfrac{3}{11} = 0,(27)$, *então* $0 + 9 = 9; 1 + 8 = 9; 2 + 7 = 9$;

(2) $\dfrac{1}{13} = 0,(076923); \dfrac{2}{13} = 0,(153846)$, *então* $076 + 923 = 999; 153 + 846 = 999$;

(3) $\dfrac{1}{17} = 0,(0588235294117647)$, *então* $05882352 + 94117647 = 99999999$;

(4) $\dfrac{2}{17} = 0,(1176470588235294)$, *então* $11764705 + 88235294 = 99999999$.

Ao considerarmos, novamente, a dízima de $\dfrac{1}{7} = 0,(142857)$, com a qual, anteriormente, verificámos que o comprimento do seu período é divisível por 2, constatamos que é também divisível por 3. Desta forma, se "partirmos" o conjunto de algarismos 142857 em três números com o mesmo comprimento, ou seja, 14, 28 e 57 e os adicionarmos temos $14 + 28 + 57 = 99$.

Esta observação motiva o seguinte resultado, que configura uma generalização do teorema de Midy (ver [19]).

Teorema 2.3.3 *Seja p um inteiro positivo, q primo $\neq 2$ e 5, p primo com q e $p < q$. Seja s a ordem de 10 módulo q e $s = ds'$, com d e s' inteiros positivos, então tem-se que $\dfrac{p}{q} = 0,(u_1u_2\cdots u_d)$, onde cada u_i (para qualquer $1 \leq i \leq d$) é da forma $a_{1i}a_{2i}\cdots a_{s'i}$ para $0 \leq a_{ji} < 10$, (para qualquer $1 \leq j \leq ds'$), $k \in \mathbb{N}$ e*

$$u_1 + u_2 + \cdots + u_d = k \times (10^{s'} - 1) \text{ com } 1 \leq k \leq d - 1.$$

Demonstração: q não divide $10^{s'}-1$, uma vez que $s' < s = ds'$ e s é o menor inteiro positivo tal que q divide $10^s - 1$. Sendo $10^{ds'} - 1 = (10^{s'} - 1)(1 + 10^{s'} + \cdots + 10^{(d-1)s'})$ e $(q, 10^{s'} - 1) = 1$ então pelo teorema 1.2.6 concluímos que q divide $1 + 10^{s'} + \cdots + 10^{(d-1)s'}$.

Assim, concluímos que $\dfrac{(1 + 10^{s'} + \cdots + 10^{(d-1)s'})p}{q}$ é inteiro. Ora,

$$\frac{(1 + 10^{s'} + \cdots + 10^{(d-1)s'})p}{q} = 0,(u_1 \cdots u_d) + u_1, (u_2 \cdots u_d u_1) + \cdots$$

$$\cdots + u_1 \cdots u_{d-1}, (u_d u_1 \cdots u_{d-1}).$$

Portanto, novamente, concluímos que:

$$0,(u_1 \cdots u_d) + 0,(u_2 \cdots u_d u_1) + \cdots + 0,(u_d u_1 \cdots u_{d-1}) \quad \text{é inteiro}$$

e, ainda, que:

$$0,(u_1 \cdots u_d) + 0,(u_2 \cdots u_d u_1) + \cdots + 0,(u_d u_1 \cdots u_{d-1}) = k, \text{ com } \ 1 \leq k \leq d-1.$$

Com efeito, sendo p primo com q então $0,(u_1 u_2 \cdots u_d) < 1$.

Sejam, então,

$$0,(u_1 \cdots u_d) = u_1(10^{-s'} + 10^{-(d+1)s'} + \cdots) + \cdots + u_d(10^{-ds'} + 10^{-(2d)s'} + \cdots)$$

$$0,(u_2 \cdots u_d u_1) = u_2(10^{-s'} + 10^{-(d+1)s'} + \cdots) + \cdots + u_1(10^{-ds'} + 10^{-(2d)s'} + \cdots)$$

$$\vdots$$

$$0,(u_d u_1 \cdots u_{d-1}) = u_d(10^{-s'} + 10^{-(d+1)s'} + \cdots) + \cdots + u_{d-1}(10^{-ds'} + 10^{-(2d)s'} + \cdots)$$

Adicionando,

$$k = (u_1 + \cdots + u_d)(10^{-s'} + 10^{-2s'} + \cdots) = (u_1 + \cdots + u_d)10^{-s'} \times \frac{1}{1 - 10^{-s'}}$$

$$k = (u_1 + \cdots + u_d)\frac{1}{10^{s'} - 1}$$

E, finalmente, $u_1 + \cdots + u_d = k(10^{s'} - 1)$. □

Exemplo 2.3.4 :

(1) $\frac{1}{13} = 0,(076923)$ *s=6 divisível por 3 (s=3s'), então* $07 + 69 + 23 = 99$.

(2) $\frac{2}{13} = 0,(153846)$ *s=6 divisível por 3 (s=3s'), então* $15 + 38 + 46 = 99$.

(3) $\frac{1}{43} = 0,(023255813953488372093)$ *s=21 divisível por 3 (s=3s'), então* $0232558 + + 1395348 + 8372093 = 9999999$.

(4) $\frac{3}{7} = 0,(428571)$ *s=6 divisível por 3 (s=3s'), então* $42 + 85 + 71 = 198 = 2 \times 99$.

(5) $\frac{1}{73} = 0,(01369863)$ *s=8 divisível por 4 (s=4s'), então* $01+36+98+63 = 99+99 = 2 \times 99$.

(6) $\frac{2}{17} = 0,(1176470588235294)$ *s=16 divisível por 4 (s=4s'), então* $1176 + 4705 + + 8823 + 5294 = 9999 + 9999 = 2 \times 9999$.

(7) $\frac{2}{17} = 0,(1176470588235294)$ *s=16 divisível por 8 (s=8s'), então* $11+76+47+05+ 88 + 23 + 52 + 94 = 99 + 99 + 99 + 99 = 4 \times 99$.

Se observarmos (5), (6) e (7) do exemplo 2.3.4, verificamos que o comprimento do período de cada uma das dízimas apresentadas é divisível por um d par, $d > 1$, e o valor de k multiplicado por s' algarismos 9 é metade de d.

Defronte esta conclusão, podemos enunciar, de uma forma geral, o resultado que se segue.

Importa realçar que este resultado possibita-nos encontrar o valor concreto de k apresentado no teorema 2.3.3, no caso de d ser par.

Teorema 2.3.5 *Seja p um inteiro positivo, q primo $\neq 2$ e 5, p primo com q e $p < q$. Seja s a ordem de 10 módulo q e $s = ds'$, com d e s' inteiros positivos e d par, então tem-se que $\frac{p}{q} = 0,(u_1u_2\cdots u_d)$, onde cada u_i (para qualquer $1 \leq i \leq d$) é da forma $a_{1i}a_{2i}\cdots a_{s'i}$ para $0 \leq a_{ji} < 10$, (para qualquer $1 \leq j \leq ds'$) e*

$$u_1 + u_2 + \cdots + u_d = \frac{d}{2} \times (10^{s'} - 1).$$

Demonstração: Suponhamos $\frac{p}{q} = 0,(u_1u_2\cdots u_{2d'}) = 0,(u'_1u'_2)$ com $d = 2d'$ e

$$\begin{cases} u'_1 = u_1 \cdots u_{d'} \\ u'_2 = u_{d'+1} \cdots u_{2d'} \end{cases}.$$

Pelo **teorema de Midy** temos que,

$$u'_1 + u'_2 = u_1 \cdots u_{d'} + u_{d'+1} \cdots u_{2d'} = \underbrace{99\cdots9}_{s'}\underbrace{99\cdots9}_{s'}\cdots\underbrace{99\cdots9}_{s'} \ (d's' \text{ algarismos } 9).$$

Como,

$$(u_{d'} + u_{2d'}) \leq 2(10^{s'} - 1) = 19\cdots98 < 19\ldots9 \ \ (\text{com } s' \text{ algarismos } 9),$$

logo,

$$(u_{d'} + u_{2d'}) = 9\cdots9 = 10^{s'} - 1.$$

Da mesma maneira, concluímos que

$$(u_i + u_{d'+i}) = 10^{s'} - 1, \quad \text{para todo} \ \ i, \quad \text{com} \ \ 1 \leq i < d'.$$

Assim, finalmente, temos

$$u_1 + u_2 + \cdots + u_{2d'} = d' \times (10^{s'} - 1), \quad \text{ou seja,}$$

$$u_1 + u_2 + \cdots + u_d = \frac{d}{2} \times (10^{s'} - 1).$$

□

Exemplo 2.3.6 :

(1) $\frac{1}{19} = 0,(052631578947368421)$ *em que* $s = 18$ *é divisível por* 6 *(par)* $s = 6 \times 3$*, logo* $d = 2 \times 3$*, então* $052 + 631 + 578 + 947 + 368 + 421 = 999 + 999 + 999 = 3 \times 999$*, ou ainda,* $052 + 631 + 578 + 947 + 368 + 421 = \frac{6}{2}(10^3 - 1)$.

(2) $\frac{1}{41} = 0,(02439048780731709756121951463426829365 85)$ *em que* $s = 40$ *é divisível por* 10*(par)* $s = 10 \times 4$*, logo* $d = 2 \times 5$*, então* $0243+9048+7807+3170+9756+1219+5146+3426+8293+6585 = 9999+9999+9999+9999+9999 = 5 \times 9999$*, ou ainda,* $0243+9048+7807+3170+9756+1219+5146+3426+8293+6585 = \frac{10}{2}(10^4-1)$.

2.4 Critérios de divisibilidade

Nesta secção estudaremos apenas alguns critérios de divisibilidade por números primos, evidenciando determinadas relações estabelecidas pelas caraterísticas dos números mencionados.

Recordando (r_i) a sucessão dos termos do resto da divisão, por exemplo, de $\frac{1}{7}$, temos o seguinte:

$$10 \equiv 3;\ \ 10^2 \equiv 9 \equiv 2;\ \ 10^3 \equiv 2 \times 3 = 6 \equiv -1;\ \ 10^4 \equiv -3;\ \ 10^5 \equiv -9 \equiv -2;$$

$$10^6 \equiv -6 \equiv 1.$$

Com efeito, podemos apresentar N um inteiro tal que

$$N = a_n + 10a_{n-1} + 10^2 a_{n-2} + 10^3 a_{n-3} + \cdots \text{ com } 0 \leq a_i < 10 \text{ e } 0 \leq i \leq n \in \mathbb{N},$$

ou seja,

$$N \equiv a_n + 3a_{n-1} + 2a_{n-2} - a_{n-3} - 3a_{n-4} - 2a_{n-5} + a_{n-6} + \cdots \mod 7,$$

o que estabelece o critério de divisibilidade por 7.

Exemplo 2.4.1 :

(1) 12345 *é divisível por* 7*?*
$1 \times 5 + 3 \times 4 + 2 \times 3 - 1 \times 2 - 3 \times 1 = 18 \equiv 4 \neq 0 \mod 7$*, logo não é divisível por* 7*.*

(2) 581126 *é divisível por* 7*?*
$1 \times 6 + 3 \times 2 + 2 \times 1 - 1 \times 1 - 3 \times 8 - 2 \times 5 = -21 \equiv 0 \mod 7$*, logo é divisível por* 7*.*

Por analogia, estabelecemos outros critérios de divisibilidade que apresentamos na tabela seguinte:

p primo	3	11	7	13	17
conj. coeficientes que estabelece o critério	1,1,1	1,-1,1,-1	1,3,2,-1,-3,-2	1,-3,-4,-1,3,4	1,-7,-2,-3,4, 6,-8,5,-1,7, 2,3,-4,-6,8,-5
comp. do conjunto coeficientes	1	2	6	6	16
dízima periódica de $\frac{1}{p}$	0,(3)	0,(09)	0,(142857)	0,(076923)	0,(0588235294 117647)
comprimento do período da dízima $\frac{1}{p}$	1	2	6	6	16

Tabela 2.2: Critérios de divisibilidade por 3, 7, 11, 13 e 17

De seguida, observemos o seguinte resultado:

Teorema 2.4.2 *Seja p primo. O comprimento do conjunto de coeficientes que estabelece o critério de divisibilidade por p é igual ao respetivo comprimento do período da dízima de $\frac{1}{p}$.*

Demonstração: Verificamos, pelo exemplo considerado no início desta secção, que o comprimento do conjunto de coeficientes que estabelece o critério é o menor número inteiro, $k_0 \neq 0$, tal que $10^{k_0} \equiv 1 \mod p$.

Consideremos, então, p primo, $p \neq 2$ e $p \neq 5$, pelo pequeno teorema de Fermat, temos $10^{p-1} \equiv 1 \mod p$ e existe um k_0 tal que $k_0 \leq p-1$.

Vamos então supor que k_1 é o comprimento do período da dízima de $\frac{1}{p}$, como sendo o menor inteiro não negativo, tal que $10^{k_1} \equiv 1 \mod p$. Logo, importa mostrar que $k_0 = k_1$.

Seja $10^{k_0} \equiv 1 \mod p$ então existe um n tal que $10^{k_0} = 1 + np$ com $n < 10^{k_0}$, donde $\frac{1}{p} = \frac{n}{10^{k_0}-1}$. Assim,

$$\begin{aligned} 10^{-k_0} + 10^{-2k_0} + 10^{-3k_0} + \cdots &= 10^{-k_0}(1 + 10^{-k_0} + 10^{-2k_0} + \cdots) \\ &= 10^{-k_0}\frac{1 - \lim_{i\to+\infty} 10^{-ik_0}}{1 - 10^{-k_0}} \\ &= \frac{10^{-k_0}}{1 - 10^{-k_0}} = \frac{1}{10^{k_0}-1}. \end{aligned}$$

Portanto, fica:

$$\frac{1}{p} = n(10^{-k_0} + 10^{-2k_0} + 10^{-3k_0} + \cdots) \quad e \quad n < 10^{k_0}.$$

Considerando $n = a_1a_2\cdots a_{k_0}$, com $a_i \in \{0, 1, \ldots, 9\}$, para $1 \leq i \leq k_0$ obtemos,

$$\begin{aligned}\frac{1}{p} &= a_1a_2\cdots a_{k_0}(10^{-k_0} + 10^{-2k_0} + 10^{-3k_0} + \cdots)\\ &= 0, a_1a_2\cdots a_{k_0} + 0, \underbrace{0\ldots0}_{k_0 zeros} a_1a_2\cdots a_{k_0} + \cdots\\ &= 0, (a_1a_2\cdots a_{k_0}),\end{aligned}$$

o que prova que o período começa logo após a vírgula e que $k_1 \leq k_0$.

Consideremos também $\frac{1}{p} = 0, a_1a_2\cdots a_{k_1}$, então $10^{k_1} \times \frac{1}{p} = a_1a_2\cdots a_{k_1} + \frac{1}{p}$, logo $10^{k_1} \equiv a_1a_2\cdots a_{k_1} \times p + 1$, donde $10^{k_1} \equiv 1 \mod p$ e, portanto, $k_1 \geq k_0$.

Concluímos que $k_1 = k_0$. □

Observação 2.4.3 *Notemos, por exemplo, que os conjuntos dos coeficientes que estabelecem os critérios de divisibilidade:*

- *por* 7*:* $1, 3, 2, -1, -3, -2$
- *por* 13*:* $1, -3, -4, -1, 3, 4$
- *por* 17*:* $1, -7, -2, -3, 4, 6, -8, 5, -1, 7, 2, 3, -4, -6, 8, -5$

são conjuntos de algarismos que se apresentam simétricos.

Perante esta observação, coloquemos uma interrogação: será que os conjuntos dos coeficientes que estabelecem os critérios de divisibilidade por números primos apresentam-se sempre simétricos?

Verifiquemos esta curiosidade.

Designemos k_0 o comprimento do conjunto dos coeficientes.

Se k_0 **é par**, e como $10^{k_0} \equiv 1 \mod p$, então $\frac{k_0}{2}$ é inteiro.

Seja $X = 10^{\frac{k_0}{2}}$, temos $X^2 \equiv 1 \mod p \iff (X-1)(X+1) \equiv 0 \mod p$.

$X = 1$ é excluído senão $10^{\frac{k_0}{2}} \equiv 1 \mod p$ e k_0 não seria o menor, por isso, consideramos $10^{\frac{k_0}{2}} \equiv -1 \mod p$ e, assim, o conjunto dos coeficientes é simétrico, tal como verificamos para os casos analisados.

Se k_0 **é ímpar** não se verifica qualquer simetria, como podemos observar considerando o exemplo do conjunto dos coeficientes associado ao número primo 31 que é o seguinte: $1, 10, 7, 8, 18, 25, 2, 20, 14, 16, 5, 19, 4, 9, 28$.

Reparemos, ainda, que 7 e 17 são primos longos. Atendendo à definição 2.2.6, se p é um número primo longo, na base 10, o comprimento do período da dízima $\frac{1}{p}$ é par. Portanto, os conjuntos dos coeficientes que estabelecem os critérios de divisibilidade por números primos longos apresentam-se sempre simétricos.

Capítulo 3

Números *teimosos*

Neste capítulo vamos estudar alguns números que designamos por números *teimosos*. Esta designação deve-se a determinadas características evidenciadas por estes números, nomeadamente, quando multiplicados por um certo valor sofrem apenas uma alteração da posição dos algarismos que os compõem.

3.1 Número n-parasítico

Vamos começar por observar os números n-parasíticos, na base 10. Vejamos, então, a sua definição:

Definição 3.1.1 (Número n-parasítico). *Sejam n e k inteiros positivos. Dizemos que $B = b_1 10^{k-1} + b_2 10^{k-2} + \cdots + b_{k-1}10 + b_k$, onde $b_1, \ldots b_k \in \{0, 1, 2, \ldots, 9\}$, é um* número n-parasítico*, se*

$$nB = b_k 10^{k-1} + b_1 10^{k-2} + \cdots + b_{k-2}10 + b_{k-1}.$$

Teorema 3.1.2 *Sejam n um inteiro positivo, $r \in \{1, 2, \ldots, 9\}$ e $k = ord_{10n-1}10$. Então $B = \dfrac{r}{10n-1} \times 10^k - 1$ é um número n-parasítico.*

Demonstração: Como $k = \mathrm{ord}_{10n-1}10$ então $(10n-1) \mid (10^k - 1)$, logo B é um inteiro positivo.

Como $10n - 1 \equiv -1 \mod 10$ então $B \equiv r(10^k - 1)(10n-1)^{-1} \equiv r \mod 10$, ou seja, se escrevermos $B = b_1 10^{k-1} + b_2 10^{k-2} + \cdots + b_{k-1}10 + b_k$, com $b_1, \ldots b_k \in \{0, 1, 2, \ldots, 9\}$, então $b_k = r$.

Mostremos agora que B é um número n-parasítico. Portanto, temos:

$$\begin{aligned} nB &= \frac{nb_k}{10n-1}(10^k-1) = \frac{10nb_k}{10n-1} \times \frac{10^k-1}{10} \\ &= \frac{(10nb_k - b_k + b_k)}{10n-1} \times \frac{10^k-1}{10} = \frac{(10n-1)b_k + b_k}{10n-1} \times \frac{10^k-1}{10} \\ &= \left(b_k + \frac{b_k}{10n-1}\right) \times \frac{10^k-1}{10}. \end{aligned}$$

Como $B = \dfrac{r}{10n-1} \times 10^k - 1$, fica:

$$\begin{aligned} nB &= \frac{B}{10} + \frac{b_k}{10}(10^k-1) \\ &= \frac{B}{10} + b_k 10^{k-1} - \frac{b_k}{10}. \end{aligned}$$

Pela definição 3.1.1, escrevemos $B = b_1 10^{k-1} + b_2 10^{k-2} + \cdots + b_{k-1}10 + b_k$, e obtemos o seguinte:

$$\begin{aligned} nB &= b_1 10^{k-2} + b_2 10^{k-3} + \cdots + b_{k-2}10 + b_{k-1} + \frac{b_k}{10} + b_k 10^{k-1} - \frac{b_k}{10} \\ &= b_k 10^{k-1} + b_1 10^{k-2} + b_2 10^{k-3} + \cdots + b_{k-2}10 + b_{k-1} \end{aligned}$$

□

Observemos, na tabela que se segue, os primeiros números n-parasíticos[1].

n	B	$n \times B$
2	105 263 157 894 736 842	210 526 315 789 473 684
3	1 034 482 758 620 689 655 172 413 793	3 103 448 275 862 068 965 517 241 379
4	102 564	410 256
5	142 857	714 285
6	10 169 491 525 423 728 813 559 932 203 389 830 508 474 576 271 186 440 677 966	61 016 949 152 542 372 881 355 993 220 338 983 050 847 457 627 118 644 067 796
7	1 014 492 753 623 188 405 797	7 101 449 275 362 318 840 579
8	1 012 658 227 848	8 101 265 822 784
9	10 112 359 550 561 797 752 808 988 764 044 943 820 224 719	91 011 235 955 056 179 775 280 898 876 404 494 382 022 471

Tabela 3.1: Os primeiros 8 números n-parasíticos

[1]No caso $n = 5$ temos que fixar $r = 7$ para obtermos $B = \dfrac{7}{49} \times 10^6 - 1 = 142857$.

3.2 Número cíclico

Continuamos na abordagem aos números *teimosos*, mas, agora, com os números cíclicos, também, na base 10. Observemos, de seguida, a sua definição:

Definição 3.2.1 (Número cíclico). *Dizemos que inteiro positivo m, com s algarismos, na base* 10*, é um* número cíclico *se quando m é multiplicado por qualquer $k \in \{2, \ldots, s\}$ obtém-se um número cujos algarismos formam uma permutação cíclica dos algarismos de m.*

Teorema 3.2.2 *Seja p um primo longo, na base* 10*, então o inteiro*

$$m = \frac{10^{p-1} - 1}{p},$$

é um número cíclico.

Demonstração: Como p é um primo longo na base 10, a ordem de 10 módulo p é $p-1$. Portanto, todos os números racionais $\frac{1}{p}, \frac{2}{p}, \ldots, \frac{p-1}{p}$ têm uma dízima infinita periódica com o mesmo período, uma vez que o número de períodos diferentes é $\frac{p-1}{\text{ord}_p 10} = 1$.

Pelo pequeno teorema de Fermat, p divide $10^{p-1} - 1$. Logo, os números

$$\frac{k(10^{p-1} - 1)}{p}, \text{ com } 2 \leq k \leq p-1,$$

são todos inteiros e, atendendo à observação 2.2.7, os seus algarismos são permutações cíclicas dos algarismos de m. □

Exemplo 3.2.3 : *Consideremos $p = 7$ primo longo, na base* 10*.*

Então, $m = \frac{10^6 - 1}{7} = 142587$.

$$2m = 285714$$
$$3m = 428571$$
$$4m = 571428$$
$$5m = 714285$$
$$6m = 857142$$

Os algarismos de $2m$, $3m$, $4m$, $5m$ e $6m$ são permutações cíclicas dos algarismos de m.

Observemos os cinco primeiros números cíclicos associados a p primos longos, na base 10:

m	p
142857	7
0588235294117647	17
052631578947368421	19
043478260869565217391	23
034482758620689655172413793	29

Vejamos, de seguida, um resultado associado ao conceito de número cíclico.

Teorema 3.2.4 *Sejam n_1 e n_2 inteiros positivos. Seja $m = \dfrac{10^{p-1}-1}{p}$ um número cíclico tal que $m = m_1 \cdots m_{p-1}$, onde $m_1, \ldots, m_{p-1} \in \{0, 1, \ldots, 9\}$, e k inteiro, onde $k \leq \dfrac{10^{2(p-1)}}{m}$. Dada a divisão de $m \times k$ por 10^{p-1} tal que $m \times k = n_1 \times 10^{p-1} + n_2$ então $m \mid n_1 + n_2$.*

Demonstração: Tomemos $x = m \times k = x_1 \cdots x_{2(p-1)}$, onde $x_1, \ldots, x_{2(p-1)} \in \{0, 1, \ldots, 9\}$, e p um número primo de modo que $k \leq \dfrac{10^{2(p-1)}}{m}$. Queremos, então, mostrar que $x_1 \cdots x_{p-1} + x_p \cdots x_{2(p-1)}$ é divisível por m. Temos então:

$$\frac{x}{10^{2(p-1)}-1} = 0, x_1 \cdots x_{2(p-1)} x_1 \cdots ,$$

e, ainda,

$$10^{p-1} \times \frac{x}{10^{2(p-1)}-1} = x_1 \cdots x_{p-1}, x_p \cdots x_{2(p-1)} x_1 \cdots .$$

Suponhamos que $n_1 + n_2$ tem $p-1$ algarismos, então podemos escrever

$$n_1 + n_2 = x_1 \cdots x_{p-1} + x_p \cdots x_{2(p-1)} = y_1 \cdots y_{p-1},$$

onde $y_1, \ldots, y_{p-1} \in \{0, 1, \ldots, 9\}$, e obtemos,

$$10^{p-1} \times \frac{x}{10^{2(p-1)}-1} = x_1 \cdots x_{p-1}, y_1 \cdots y_{p-1} y_1 \cdots ,$$

ou

$$10^{p-1} \times \frac{x}{10^{2(p-1)}-1} = \frac{x}{10^{p-1}-1} = \frac{m \times k}{10^{p-1}-1} = k \times \frac{1}{p}.$$

Assim, $y_1 \cdots y_{p-1} y_1 \cdots$ é múltiplo de $\frac{1}{p}$, ou seja, $y_1 \cdots y_{p-1}$ é divisível por m. Portanto $n_1 + n_2$ é divisível por m. E, assim, obtemos:

$$n_1 = \left[\frac{k}{p}\right] \qquad n_2 = m \times k - 10^{p-1} \times \left[\frac{k}{p}\right].$$

□

Exemplo 3.2.5 :

(1) *Consideremos* $m = 142857$ *um número cíclico associado ao primo longo* 7 *e* $k = 888$

$$m \times k = 142857 \times 888 = 126857016 \qquad \rightarrow \qquad 126 + 857016 = 857142$$

Verificamos que $m \mid 857142$.

(2) *Consideremos* $m = 0588235294117647$ *um número cíclico associado ao primo longo* 17 *e* $k = 142857$

$$m \times k = 0588235294117647 \times 142857 = 84033529411764707479$$

$$8403 + 3529411764707479 = 3529411764705882$$

Verificamos que $m \mid 3529411764705882$.

Corolário 3.2.6 *Seja* $k > \dfrac{10^{2(p-1)}}{m}$. *Seja* n_i *o número de "partes" de* $m \times k$, *onde* $i = \left[\dfrac{[log(m \times k)]}{p-1}\right] + 1$, *então* $m \mid \sum_i n_i$.

Exemplo 3.2.7 :

(1) *Consideremos* $m = 142857$ *e* $k = 7000008$.

$$Calculando\ i = \left[\frac{[log(142857 \times 7000008)]}{6}\right] + 1 = 3.$$

$$m \times k = 142857 \times 7000008 = 1000000142856$$

$$1 + 000000 + 142856 = 142857$$

Claramente, $m \mid 142857$.

(2) *Consideremos* $m = 0588235294117647$ *e* $k = 190000000000000000$.

$$Calculando\ i = \left[\frac{[log(0588235294117647 \times 190000000000000000)]}{16}\right] + 1 = 3.$$

$$m \times k = 0588235294117647 \times 190000000000000000 =$$

$$= 011176470588235293000000000000000000$$

$$01 + 1176470588235293 + 0000000000000000 = 1176470588235303$$

Verificamos que $m \mid 1176470588235303$.

3.3 Números *teimosos* em diferentes bases

Vamos agora abordar os conceitos de número n-parasítico e de número cíclico em diferentes bases numéricas.

Comecemos por apresentar para um número n-parasítico a seguinte definição:

Definição 3.3.1 (Número n-parasítico em b). *Sejam n e k inteiros positivos. Seja b uma base numérica ($b > 1$). Dizemos que $\beta = d_1 b^{k-1} + d_2 b^{k-2} + \cdots + d_{k-1} b + d_k$ onde $d_1, \ldots d_k \in \{0, 1, 2, \ldots, b-1\}$, é um* número n-parasítico, *se $n\beta = d_k b^{k-1} + d_1 b^{k-2} + \cdots + d_{k-2} b + d_{k-1}$.*

Teorema 3.3.2 *Sejam n e k inteiros positivos, $r \in \{1, 2, \ldots, b-1\}$ e $k = ord_{bn-1} b$, onde representa b uma base numérica ($b > 1$). Então $\beta = \frac{r}{bn-1} \times b^k - 1$ é um número n-parasítico.*

A demonstração deste resultado não será aqui considerada, pelo facto de ser semelhante à do teorema 3.1.2, diferindo apenas na utilização da base numérica b.

Exemplo 3.3.3 :

(1) *Consideremos* $b = 5$, $r = 3$ *e* $n = 4$. *Obtemos* $k = ord_{19}5 = 9$.

Portanto,

$$\beta = \frac{3}{5 \times 4 - 1} \times 5^9 - 1 = (308388)_{10}$$
$$= (034332023)_5$$

Então,

$$n\beta = 4_{10} \times (308388)_{10} = (1953124)_{10}$$
$$= (303433202)_5$$

(2) *Consideremos* $b = 7$, $r = 5$ *e* $n = 5$. *Obtemos* $k = ord_{34}7 = 16$.

Portanto,

$$\beta = \frac{5}{7 \times 5 - 1} \times 7^{16} - 1 = (4887195672000)_{10}$$
$$= (1013042146536245)_7$$

Então,

$$n\beta = 5_{10} \times (4887195672000)_{10} = (24435978360000)_{10}$$
$$= (5101304214653624)_7$$

(3) *Consideremos* $b = 16$, $r = 11$ *e* $n = 7$. *Obtemos* $k = ord_{111}16 = 9$.

Portanto,

$$\beta = \frac{11}{16 \times 7 - 1} \times 16^9 - 1 = (6810038235)_{10}$$
$$= (195E8EFDB)_{16}$$

Então,

$$n\beta = 7_{10} \times (6810038235)_{10} = (47670267645)_{10}$$
$$= (B195E8EFD)_{16}$$

Relativamente ao número cíclico, apresentamos a definição seguinte:

Definição 3.3.4 (Número cíclico em b). *Dizemos que um inteiro positivo μ, com s algarismos, numa base b $(b > 1)$, é um* número cíclico *se quando μ é multiplicado por qualquer $k \in \{2, \ldots, s\}$ obtém-se um número cujos algarismos formam uma permutação cíclica dos algarismos de μ.*

Teorema 3.3.5 *Seja p um primo longo em b, onde b representa uma base numérica $(b > 1)$, então o inteiro*

$$\mu = \frac{b^{p-1} - 1}{p},$$

é um número cíclico.

A demonstração deste resultado não será aqui considerada, pelo facto de ser semelhante à do teorema 3.2.2, diferindo apenas na utilização da base numérica b.

Exemplo 3.3.6 :

(1) *Consideremos $b = 2$, $p = 5$ primo longo em $b = 2$.*

Portanto,

$$\begin{aligned} \mu = \frac{2^4 - 1}{5} &= (3)_{10} \\ &= (0011)_2 \end{aligned}$$

Então,

$$\begin{aligned} 2\mu &= 6_{10} = (0110)_2 \\ 3\mu &= 9_{10} = (1001)_2 \\ 4\mu &= 12_{10} = (1100)_2 \end{aligned}$$

são números cujos algarismos formam uma permutação cíclica dos algarismos de μ.

(2) *Consideremos $b = 3$, $p = 17$ primo longo em $b = 3$.*

Portanto,

$$\begin{aligned} \mu = \frac{3^{16} - 1}{17} &= (2532160)_{10} \\ &= (0011202122110201)_3 \end{aligned}$$

Então,

$$\begin{aligned} 2\mu = 5064320_{10} &= (0100112021221102)_3 \\ 3\mu = 7596480_{10} &= (0112021221102010)_3 \\ \vdots \qquad &\quad \vdots \\ 15\mu = 37982400_{10} &= (2122110201001120)_3 \\ 16\mu = 40514560_{10} &= (2211020100112021)_3 \end{aligned}$$

são números cujos algarismos formam uma permutação cíclica dos algarismos de μ*.*

(3) *Consideremos* $b = 8$*,* $p = 11$ *primo longo em* $b = 8$*.*

Portanto,

$$\begin{aligned} \mu = \frac{8^{10} - 1}{11} &= (97612893)_{10} \\ &= (0564272135)_8 \end{aligned}$$

Então,

$$\begin{aligned} 2\mu = 195225786_{10} &= (1350564272)_8 \\ 3\mu = 292838679_{10} &= (2135056427)_8 \\ \vdots \qquad &\quad \vdots \\ 9\mu = 878516037_{10} &= (6427213505)_8 \\ 10\mu = 976128930_{10} &= (7213505642)_8 \end{aligned}$$

são números cujos algarismos formam uma permutação cíclica dos algarismos de μ*.*

3.4 Números n-cíclicos

Reparemos, agora, para outros números cíclicos com ordem superior a 1 associados a números primos cujo número de períodos diferentes é igual a 2.

Vejamos a seguinte definição:

Definição 3.4.1 (Número 2-cíclico). *Dizemos que inteiro positivo* m_2*, com* t *algarismos, na base* 10*, é um* número 2-cíclico *ou um* número cíclico de ordem 2 *se quando*

m_2 é multiplicado por $k \in \{2, \ldots, 2t\}$ obtém-se um número cujos algarismos formam permutações cíclicas dos algarismos de m_2 e $2m_2$.

Teorema 3.4.2 *Seja p um primo tal que a ordem 10 módulo p é $\frac{p-1}{2}$ então o inteiro*

$$m_2 = \frac{10^{\frac{p-1}{2}} - 1}{p},$$

é um número 2-cíclico.

Exemplo 3.4.3 : *Seja o número cíclico de ordem 2 associado ao número primo 13, tal que $m_2 = 076923$ e $2m_2 = 153846$. Se multiplicarmos m_2 por $k \in \{2, \ldots, 12\}$ obtemos m_2' e $2m_2'$ cujos algarismos são permutações cíclicas de m_2 e $2m_2$, respetivamente, conforme a seguir verificamos.*

$m_2 \times k$	m_2'	$2m_2'$
$076923 \times 2 =$		153846
$076923 \times 3 =$	230769	
$076923 \times 4 =$	307692	
$076923 \times 5 =$		384615
$076923 \times 6 =$		461538
$076923 \times 7 =$		538461
$076923 \times 8 =$		615384
$076923 \times 9 =$	692307	
$076923 \times 10 =$	769230	
$076923 \times 11 =$		846153
$076923 \times 12 =$	923076	

Outros números primos que estão associados a números 2-cíclicos: 31, 43, 67, 71, 83, 89, ...

Após termos particularizado para o caso de um número cíclico de ordem 2, com o intuito de promover um melhor entendimento da noção de número cíclico de ordem n, procedemos, de seguida, à apresentação deste conceito.

Definição 3.4.4 (Número n-cíclico). *Dizemos que inteiro positivo m_n, com t algarismos, na base 10, é um* número n-cíclico *ou um* número cíclico de ordem n *se, quando m_n é multiplicado por $k \in \{2, \ldots, n \times t\}$ obtém-se um número cujos algarismos formam permutações cíclicas dos algarismos de um dos números $i \times m_n$, para algum i, $1 \leq i \leq n$.*

Teorema 3.4.5 *Seja p um primo tal que a ordem 10 módulo p é $\frac{p-1}{n}$ então o inteiro*

$$m_n = \frac{10^{\frac{p-1}{n}} - 1}{p},$$

é um número n-cíclico.

A demonstração deste resultado não será aqui considerada, pelo facto de ser semelhante à do teorema 3.2.2, apenas, neste caso, bastará atender aos vários períodos diferentes que se obtém para as dízimas das frações $\frac{1}{p}, \frac{2}{p}, \ldots, \frac{p-1}{p}$.

Exemplo 3.4.6 : *Seja o número cíclico de ordem 8 associado ao número 41 primo, tal que $m_8 = 02439$, $2m_8 = 04878$, $3m_8 = 07317$, $4m_8 = 09756$, $5m_8 = 12195$, $6m_8 = 14634$, $11m_8 = 26829$ e $15m_8 = 36585$. Se multiplicarmos m_8 por $k \in \{2, \ldots, 40\}$ obtemos m'_8, $2m'_8$, $3m'_8$, $4m'_8$, $5m'_8$, $6m'_8$, $11m'_8$ e $15m'_8$ cujos algarismos são permutações cíclicas de m_8, $2m_8$, $3m_8$, $4m_8$, $5m_8$, $6m_8$, $11m_8$ e $15m_8$ respetivamente, conforme verificamos na tabela.*

$m_8 \times k$	m'_8	$2m'_8$	$3m'_8$	$4m'_8$	$5m'_8$	$6m'_8$	$11m'_8$	$15m'_8$
02439×2		04878						
02439×3			07317					
02439×4				09756				
02439×5					12195			
02439×6						14634		
02439×7			17073					
02439×8					19512			
02439×9					21951			
02439×10	24390							
02439×11							26829	
02439×12							29268	
02439×13			31707					
02439×14						34146		
02439×15								36585
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
02439×40				97560				

Observemos na tabela seguinte a ordem n dos números cíclicos associada ao número primo p, sendo que no caso de $n = 1$ temos um primo longo. De notar, ainda, que

apresentamos apenas o menor número p.

ordem n	1	2	3	4	5	6	7	8	9	10	11	12
menor p	7	13	103	53	11	79	211	41	73	281	353	37

Tabela 3.2: A ordem n associada ao menor número primo p

Observação 3.4.7 *Podemos reparar da tabela, que a ordem n associada ao número primo p corresponde ao número de períodos diferentes de uma fração irredutível cujo denominador é esse número primo p.*

Capítulo 4

Como Ganhar no Momento Certo

Tal como no capítulo 9 do Hardy e Wright (ver [15]), onde os autores estudaram jogos combinatórios utilizando a representação de números na base binária, também, neste capítulo, iremos proceder do mesmo modo. Assim, apresentamos alguns jogos combinatórios sob a perspectiva de encontrar uma estratégia vencedora, onde o foco, para a prossecução de tal desígnio, se centra na abordagem de uma operação aritmética especial, a adição-Nim, consubstanciada na representação numérica binária.

4.1 Conceitos fundamentais

Nesta secção, vamos introduzir algumas noções importantes que se relacionam com os jogos combinatórios, das quais faremos um uso frequente ao longo deste capítulo.

Definição 4.1.1 (Jogo combinatório). *Um jogo combinatório é um jogo que apresenta as seguintes características:*

(a) *É jogado por dois jogadores, sendo que os mesmos jogam alternadamente;*

(b) *É um jogo finito, ou seja, o jogo sempre termina após um número finito de movimentos, e ainda, em cada jogada, o jogador escolhe uma entre uma quantidade finita de movimentos possíveis;*

(c) *É imparcial, ou seja, ambos os jogadores têm as mesmas possibilidades de movimentos;*

(d) *É um jogo de informação completa, ou seja, não existem informações escondidas;*

(e) *É determinístico, no sentido de que cada movimento origina uma única posição, e não há aleatoriedade (como no lançamento de dados);*

(f) *O jogo termina quando é atingida uma certa posição, a partir da qual não há mais movimentos possíveis;*

(g) *Sob a regra normal de jogo, estabelece que o último jogador a executar um movimento possível vença.*

(h) *Sob a regra misère, estabelece que o último jogador a executar um movimento possível perca.*

Ao longo deste texto consideraremos apenas jogos combinatórios com a regra normal de jogo. Destacamos, ainda, a seguinte definição:

Definição 4.1.2 (Posição terminal). *Dizemos que uma posição num jogo combinatório é uma* posição terminal *se nenhum movimento a partir dela é possível.*

Exemplo 4.1.3 : *Vejamos a seguir um exemplo de um jogo combinatório: Consideremos uma pilha com* 21 *feijões. Um movimento de cada um dos dois jogadores, que designaremos como jogador A e jogador B, consiste em retirar da pilha um, dois ou três feijões, e os jogadores realizam estes movimentos alternadamente. Assim, o jogador A começa o jogo e o vencedor é aquele que retira o último feijão da pilha. Reparemos que existe uma estratégia vencedora para o jogador que efetuar o primeiro movimento. Deste modo, o jogador A retira um feijão, deixando* 20 *feijões na pilha. Após o movimento do jogador B, o jogador A retira tantos feijões quantos forem necessários, de modo a deixar* 16 *feijões na pilha. Continuando desta forma, o jogador A deixará, após cinco rodadas,* 4 *feijões na pilha. Considerando que o jogador B pode retirar no máximo* 3 *feijões, o próximo movimento do jogador A será retirar todos os restantes feijões, o que permitirá a sua vitória. Portanto, a estratégia vencedora consiste em deixar um número de feijões para o jogador B, que seja múltiplo de* 4*.*

Definição 4.1.4 (V-posição e D-posição). *Dizemos que uma posição de um jogo combinatório é uma* V[1]-posição *(posição vencedora) se houver uma sequência de movimentos que permitam ao jogador que realizou o último movimento, vencer o jogo, quaisquer que sejam os movimentos que o seu adversário faça. Uma posição é uma* D[2]-posição *se não for uma V-posição.*

[1] V de vitória
[2] D de derrota

No exemplo 4.1.3, observamos que as pilhas com quantidades de feijões que são múltiplas de 4 são as V-posições, enquanto as restantes são D-posições.

Podemos estabelecer as seguintes propriedades para um jogo combinatório com regra normal de jogo.

Proposição 4.1.5 **(ver[11])** *Dado um jogo combinatório, então:*

(a) *a posição terminal é uma V-posição.*

(b) *a partir de qualquer D-posição, existe, pelo menos, um movimento que origina uma V-posição.*

(c) *a partir de uma V-posição, todo o movimento origina uma D-posição.*

De salientar que iremos estudar jogos combinatórios para os quais esta proposição vai ser demonstrada, como no caso do jogo Nim, que se segue na próxima secção.

4.2 O Jogo Nim: a adição-Nim

O jogo Nim foi o primeiro jogo combinatório a ser tratado matematicamente, em 1902, pelo matemático Bouton. Este matematico apresentou uma teoria para a estratégia vencedora do jogo ligada à aritmética dos números naturais no sistema de numeração binário.

Trata-se de um jogo com diversas variantes, portanto, encontramos as mais diversas regras quanto à quantidade de objetos utilizados no jogo, ao número de pilhas e à quantidade de objetos por pilha, assim como, poder ou não determinar-se um limite máximo de objetos que podem ser retirados em cada movimento.

O Nim, na sua variante mais clássica, é um jogo para dois jogadores que se joga com pilhas de objetos. Em cada movimento, cada jogador escolhe uma pilha e retira dela o número de objetos que desejar. De salientar que um jogador só pode tirar objetos de uma única pilha e tem que tirar pelo menos um objeto. Ganha o jogador que retirar o último objeto.

Por exemplo, se o jogo envolver apenas uma pilha de feijões, a caracterização é muito simples. Se a pilha não for vazia, o próximo jogador ganha, retirando todos os feijões. Se a coluna for vazia, o jogador anterior ganhou.

Ilustrando o jogo temos o seguinte:

Número de objetos (feijões)	0	1	2	3	4	...
Tipo de posição	V	D	D	D	D	...

Com duas pilhas, o jogo também não é difícil. Se as pilhas forem diferentes, o jogador seguinte iguala-as e, a partir daqui, copia a jogada do adversário. Por exemplo, se duas pilhas, com 4 e 6 feijões, forem representadas pelo par $(4, 6)$, então a melhor jogada é para $(4, 4)$. Assim, a caracterização das posições do Nim com duas pilhas, pode representar-se por (n, m) com $\{\text{V se } n = m;\ \text{D se } n \neq m\}$.

No caso de três pilhas a análise não é tão simples. Necessitamos de novos conceitos para determinar a melhor estratégia, ou seja, a estratégia vencedora, conceitos esses que também se podem aplicar nos casos de uma ou duas pilhas.

A "nova" operação que necessitamos para caracterizar as posições do Nim designa-se por **adição-Nim** e podemos defini-la assim:

Definição 4.2.1 (Adição-Nim). *Dados* $p = p_n 2^n + p_{n-1}2^{n-1} + \cdots + p_1 2^1 + p_0 2^0$ *e*

$$q = q_n 2^n + q_{n-1}2^{n-1} + \cdots + q_1 2^1 + q_0 2^0,$$

onde p_i, $q_i \in \{0, 1\}$, *para* $i \in \{0, 1, \ldots, n\}$, *definimos a* adição-Nim *de* p *e* q *e representamos por* $p \oplus q$, *como sendo,*

$$p \oplus q = y_n 2^n + \cdots + y_1 2^1 + y_0,$$

onde

$$y_i = \begin{cases} 0 & \text{se } q_i = p_i \\ 1 & \text{se } q_i \neq p_i. \end{cases}$$

Em suma, a soma-Nim de duas potências de 2 é simplesmente a soma usual quando estas são diferentes e é zero quando são iguais.

Teorema 4.2.2 *O conjunto dos números naturais forma com a adição-Nim um grupo abeliano.*

Facilmente vemos que a adição-Nim é associativa, comutativa, tem elemento neutro que é o zero e todos os elementos têm oposto (o oposto de um elemento é o próprio elemento).

Importa, agora, mostrarmos que é válida a **lei do corte**:

Dados p, q e r quaisquer, definidos em 4.2.1, então:

$$\begin{aligned} p \oplus q = r \oplus q &\Leftrightarrow (p \oplus q) \oplus q = (r \oplus q) \oplus q && \text{pela definição de adição-Nim} \\ &\Leftrightarrow p \oplus (q \oplus q) = r \oplus (q \oplus q) && \text{pela associatividade da adição-Nim} \\ &\Leftrightarrow p \oplus 0 = r \oplus 0 && \text{por definição de inverso de um elemento} \\ &\Leftrightarrow p = r && \text{por definição de elemento neutro} \end{aligned}$$

Exemplo 4.2.3 :

(1) *A soma-Nim de* 6 *e* 5 *obtemo-la notando que* $6 = 2^2 + 2^1$*;* $5 = 2^2 + 2^0$*, e, portanto,* $6 \oplus 5 = (2^2 + 2^1) \oplus (2^2 + 2^0) = (2^2 \oplus 2^2) \oplus (2^1 \oplus 2^0) = 2^1 + 2^0 = 2 + 1 = 3$.

(2) $12 \oplus 21 = (2^3 + 2^2) \oplus (2^4 + 2^2 + 2^0) = 16 + 8 + 1 = 25$.

Esta operação *diferente* ganhou importância, porque Bouton (ver [23]) provou, em 1902, que se conseguirmos deixar ao adversário pilhas de objetos cujas quantidades tenham soma-Nim nula, ou seja, desde que façamos um movimento para uma posição cuja soma-Nim dos números de objetos das pilhas seja nula, ganharíamos.

Importa, neste momento, salientarmos que se considerarmos um jogo Nim com n pilhas em que, num determinado instante do jogo, a pilha i tem $p_i \in \mathbb{N}$ objetos, com $i \in \{1, \ldots, n\}$, a posição nesse instante é representada por $(p_1, p_2, \ldots, p_n)$.

Apresentamos, agora, o resultado provado por Bouton, onde é estabelecido uma caracterização para as V-posições do jogo Nim:

Teorema 4.2.4 (Teorema de Bouton). *Uma posição* $(p_1, p_2, \ldots, p_n)$ *no jogo Nim é uma V-posição se e só se* $p_1 \oplus p_2 \oplus \cdots \oplus p_n = 0$.

Demonstração: Iremos ter por base a Proposição 4.1.5. Qualquer posição ou é V-posição ou é D-posição. Seja $\mathcal{V}$ o conjunto de todas as posições com soma-Nim nula e seja $\mathcal{D}$ o conjunto de todas as posições cuja soma-Nim é não nula. Então:

(1) A posição terminal pertence a $\mathcal{V}$, sendo a posição terminal $(0, 0, \ldots, 0)$ então $0 \oplus 0 \oplus \cdots \oplus 0 = 0$.

(2) Provemos que, dada uma posição de $\mathcal{V}$, qualquer movimento nessa posição altera-a para uma posição de $\mathcal{D}$. Seja então $(p_1, p_2, \ldots, p_n) \neq 0$ e $(p_1, p_2, \ldots, p_n) \in \mathcal{V}$. Sem

perda de generalidade, suponhamos que são retirados objetos da primeira pilha e obtemos a posição $(p_1', p_2, \ldots, p_n)$. Se $p_1 \oplus p_2 \oplus \cdots \oplus p_n = 0 = p_1' \oplus p_2 \oplus \cdots \oplus p_n$ então, pela lei do corte, $p_1 = p_1'$, o que é absurdo! Logo $(p_1', p_2, \ldots, p_n) \neq 0$ e, portanto, obtemos $(p_1', p_2, \ldots, p_n) \in \mathcal{D}$.

(3) Falta provar que, dada uma posição de $\mathcal{D}$, existe sempre um movimento que a transforma numa posição de $\mathcal{V}$.

Seja $(p_1, p_2, \ldots, p_n) \in \mathcal{D}$. Seja $N = p_1 \oplus p_2 \oplus \cdots \oplus p_n$ e suponhamos N na base 2 é da forma $N = (N_s, N_{s-1}, \ldots, N_1, N_0)_2$, onde $N_0, \ldots, N_s \in \{0, 1\}$.

Consideremos d tal que $N_d = 1$ e se $N_b = 1$ então $b \leq d$. Assim, temos que d é o dígito 1 mais à esquerda da representação binária de N. Tomemos um $k \in \{1, \ldots, n\}$ de forma que o d-ésimo dígito de p_k seja também 1. k existe uma vez que o dígito N_d é a soma-Nim dos d-ésimos dígitos de cada p_i. Consideremos $q_k = N \oplus p_k$. Então $q_k < p_k$, uma vez que todos os dígitos à esquerda de d são os mesmos em p_k e q_k e são nulos e, ainda, o d-ésimo dígito em q_k passa de 1 para 0. Vamos provar que se retirarmos $p_k - q_k$ objetos da pilha k, obtemos uma posição cuja soma-Nim é nula.

A posição obtida após este movimento é $(p_1, \ldots, p_{k-1}, q_k, p_{k+1}, \ldots, p_n)$, onde

$$q_k = N \oplus p_k = p_1 \oplus \cdots \oplus p_{k-1} \oplus p_{k+1} \oplus \cdots \oplus p_n,$$

logo

$$p_1 \oplus \cdots \oplus q_k \oplus p_{k+1} \oplus \cdots \oplus p_n = N \oplus p_k \oplus q_k = N \oplus p_k \oplus (N \oplus p_k) = 0.$$

Portanto, obtemos uma posição de $\mathcal{V}$.

□

Exemplo 4.2.5 *Consideremos o jogo Nim com a seguinte posição,* $(7, 5, 3, 2)$. *Vamos fazer a adição-Nim.*

7	1	1	1	
5	1	0	1	
3	0	1	1	
2	0	1	0	
$soma - Nim$	0	1	1	$= 3$

Portanto, uma D-posição.

A coluna mais significante com um número ímpar de dígitos 1 *é a segunda. Assim, temos, exatamente, três possíveis V-posições, que são as seguintes:*

- *retirar da primeira pilha* 3 *objetos:*

4	1	0	0	
5	1	0	1	
3	0	1	1	
2	0	1	0	
$soma - Nim$	0	0	0	$= 0$

- *retirar da terceira pilha todos os objetos:*

7	1	1	1	
5	1	0	1	
0	0	0	0	
2	0	1	0	
$soma - Nim$	0	0	0	$= 0$

- *retirar da última pilha* 1 *objeto:*

7	1	1	1	
5	1	0	1	
3	0	1	1	
1	0	0	1	
$soma - Nim$	0	0	0	$= 0$

4.3 A Função de Sprague-Grundy

Associada ao jogo Nim, temos uma importante teoria, designada por Teoria de Sprague-Grundy desenvolvida para todos os jogos combinatórios, mas que não será objeto de desenvolvimento nesta dissertação. Contudo, apresentaremos aqui algumas definições e resultados básicos decorrentes dessa teoria, que nos permitirão o desenvolvimento, de forma mais cuidada, da matéria que se segue.

Comecemos, então, por enunciar a seguinte definição:

Definição 4.3.1 (Nímero mínimo excluído). *Dado um conjunto finito de números* $\mathbb{S} \subset \mathbb{N}_0$*, definimos o* nímero[3] mínimo excluído*,* $mex(\mathbb{S})$*, como sendo*

$$mex(\mathbb{S}) = min\{i \in \mathbb{N}_0 : i \notin \mathbb{S}\}.$$

Salienta-se, ainda, que $\text{mex}(\emptyset) = 0$.

Enunciamos, de seguida, para qualquer jogo combinatório, a definição de função de Sprague-Grundy:

Definição 4.3.2 (Função de Sprague-Grundy). *Dado um jogo combinatório qualquer, a* função de Sprague-Grundy *associada a este jogo é a função que, a cada posição* P *do jogo, associa um inteiro não negativo que designamos por nímero da posição* P*. Denotamos por* $g(P)$ *a* função de Sprague-Grundy *associada à posição* P *do jogo.*

Apresentamos para um jogo Nim, a seguinte definição:

Definição 4.3.3 (Função de Sprague-Grundy associada ao jogo Nim). *Dado um jogo Nim, a* função de Sprague-Grundy $g(P)$ *associada a este jogo, que a cada posição* P *do jogo, associa um nímero da posição* P*, é definida,*

$$g(P) = \text{mex}(\{g(Q) : Q \in \mathcal{G}\}), \tag{4.1}$$

onde $\mathcal{G}$ *representa todas as posições que podem ser alcançadas a partir de* P*, após um só movimento possível.*

Exemplo 4.3.4 : *Relativamente ao exemplo 4.1.3, verifiquemos a função de Sprague-Grundy, definida em 4.1, para uma pilha com* 21 *feijões da seguinte forma:*

- *Pilha com* 0 *feijões,* $g(0) = mex(\{\emptyset\}) = 0$
- *Pilha com* 1 *feijão,* $g(1) = mex(\{g(0)\}) = mex(\{0\}) = 1$
- *Pilha com* 2 *feijões,* $g(2) = mex(\{g(1), g(0)\}) = mex(\{1, 0\}) = 2$
- *Pilha com* 3 *feijões,* $g(3) = mex(\{g(2), g(1), g(0)\}) = mex(\{2, 1, 0\}) = 3$

[3] Combinação de Nim com número

- *Pilha com* 4 *feijões,* $g(4) = mex(\{g(3), g(2), g(1)\}) = mex(\{3, 2, 1\}) = 0$
- *Pilha com* 5 *feijões,* $g(5) = mex(\{g(4), g(3), g(2)\}) = mex(\{0, 3, 2\}) = 1$
- *Pilha com* 6 *feijões,* $g(6) = mex(\{g(5), g(4), g(3)\}) = mex(\{1, 0, 3\}) = 2$
- *Pilha com* 7 *feijões,* $g(7) = mex(\{g(6), g(5), g(4)\}) = mex(\{2, 1, 0\}) = 3$
- *Pilha com* 8 *feijões,* $g(8) = mex(\{g(7), g(6), g(5)\}) = mex(\{3, 2, 1\}) = 0$

$$\vdots$$

- *Pilha com* 20 *feijões,* $g(20) = mex(\{g(19), g(18), g(17)\}) = mex(\{3, 2, 1\}) = 0$
- *Pilha com* 21 *feijões,* $g(21) = mex(\{g(20), g(19), g(18)\}) = mex(\{0, 3, 2\}) = 1$

Constatamos, claramente, que $g(n + 4) = g(n) = n \mod 4$, $\forall n \in \{0, 1, \ldots, 21\}$.

Portanto, a estratégia é deixar um número de feijões, para o adversário, que seja múltiplo de 4.

Observemos o seguinte resultado:

Teorema 4.3.5 (ver[3, 6, 8]) *Dado um jogo combinatório, existe uma estratégia vencedora para o jogador que começa o jogo a partir de uma certa posição se e só se o número dessa posição é maior ou igual a* 1.

Notemos que o teorema 4.2.4 (teorema de Bouton) é uma consequência do teorema 4.3.5, uma vez que no jogo Nim, se o jogador que começa o jogo, a partir de uma certa posição, fizer um movimento para uma posição cuja soma-Nim dos números de objetos das pilhas seja nula, vence o jogo.

Importa apresentarmos antes de finalizarmos esta secção a seguinte definição:

Definição 4.3.6 *Sejam* n *jogos combinatórios* $J_1, \ldots, J_n$. *Dados dois jogadores que jogam alternadamente e escolhendo um jogo* J_i, $i \in \{1, 2, \ldots, n\}$, *por forma a realizar um movimento possível, determinado por este jogo. O jogo termina quando não houver mais movimentos possíveis em qualquer dos* n *jogos e o vencedor é o que realizou o último movimento. Dizemos que* J_i, $i \in \{1, 2, \ldots, n\}$ *é o jogo soma dos jogos* $J_1, \ldots, J_n$.

Observação 4.3.7 (ver[8]) *O jogo Nim pode ser definido como uma soma de n jogos Nim, onde cada jogo corresponde a uma única pilha, sendo n o número de pilhas do jogo.*

O resultado (ver[3, 6, 8]) que a seguir anunciamos concede-nos a forma de obtermos a função de Sprague-Grundy da soma de n jogos combinatórios.

Proposição 4.3.8 *Sejam $J_1, \ldots, J_n$ jogos combinatórios. Se $P = (p_1, \ldots, p_n)$ é uma posição de jogo para a soma dos jogos $J_1, \ldots, J_n$, sendo p_i uma posição de jogo para J_i, então a função de Sprague-Grundy em P é dada pela soma-Nim,*

$$g(P) = g(p_1) \oplus g(p_2) \oplus \cdots \oplus g(p_n).$$

Aplicando o resultado anterior ao caso do jogo Nim sobre n pilhas, podemos afirmar que, se $P = (p_1, \ldots, p_n)$ é uma posição do jogo, então $g(P) = p_1 \oplus \cdots \oplus p_n$.

Vamos demonstrar, facilmente, este resultado por indução em p. Assim, para $p = 0$ o resultado verifica-se de forma trivial, tendo em conta o definido em 4.1 temos $g(0) = 0$.

Seja P a posição de um jogo Nim com p feijões numa só pilha, então $g(P) = p$. Por 4.1, podemos concluir,

$$g(P) = mex\{g(0), \ldots, g(P-1)\},$$

então por hipótese de indução,

$$g(P) = mex\{0, \ldots, p-1\} = p,$$

o que demonstra o resultado.

Exemplo 4.3.9 *Consideremos o jogo Nim com 4 pilhas, com 1, 3, 5 e 7 feijões, respetivamente. Verifiquemos para este jogo que a função de Sprague-Grundy associada à posição $(1, 2, 1, 0)$ tem nímero 2, atendendo a 4.1.*

Temos $g(0, 0, 0, 0) = 0$, ou seja, o nímero da posição $(0, 0, 0, 0)$ é 0. O nímero das posições $(1, 0, 0, 0)$, $(0, 1, 0, 0)$, $(0, 0, 1, 0)$ e $(0, 0, 0, 1)$ é 1 para todas, bem como o nímero das posições $(2, 0, 0, 0)$, $(0, 2, 0, 0)$, $(0, 0, 3, 0)$ e $(0, 0, 0, 4)$ é para todas 2 e, assim sucessivamente.

Temos, ainda, o seguinte:

- $g(1, 1, 0, 0) = mex\{g(1, 0, 0, 0), g(0, 1, 0, 0)\} = mex\{1, 1\} = 0$
- $g(1, 0, 1, 0) = mex\{g(1, 0, 0, 0), g(0, 0, 1, 0)\} = mex\{1, 1\} = 0$

- $g(1,0,0,1) = mex\{g(1,0,0,0), g(0,0,0,1)\} = mex\{1,1\} = 0$
- $g(1,1,1,0) = mex\{g(1,1,0,0), g(1,0,1,0), g(0,1,1,0)\} = mex\{0,0,0\} = 1$
- $g(1,2,0,0) = mex\{g(0,2,0,0), g(1,1,0,0), g(1,0,0,0)\} = mex\{2,0,1\} = 3$
- $g(0,2,1,0) = mex\{g(0,1,1,0), g(0,0,1,0), g(0,2,0,0)\} = mex\{0,1,2\} = 3,$

então,

- $g(1,2,1,0) = mex\{g(0,2,1,0), g(1,1,1,0), g(1,0,1,0), g(1,2,0,0)\} =$
  $= mex\{3,1,0,3\} = 2$

  Pela proposição 4.3.8, temos

$$g(1,2,1,0) = g(1) \oplus g(2) \oplus g(1) \oplus g(0) = 1 \oplus 2 \oplus 1 \oplus 0 = 2.$$

Na secção seguinte, apresentamos alguns jogos combinatórios, designadamente algumas variações do jogo Nim, onde destacaremos a operação adição-Nim na descoberta da estratégia vencedora.

4.3.1 Aplicações: variações do jogo Nim

Atendendo ao aludido em toda a secção anterior, analisaremos algumas variações do jogo Nim.

Exemplo 4.3.10 : *Num jogo Nim, sob a regra normal de jogo, os jogadores podem retirar apenas* 1 *ou* 4 *feijões da pilha escolhida. Portanto, verifiquemos a função de Sprague-Grundy, definida em 4.1, da seguinte forma:*

- *Pilha com* 0 *feijões,* $g(0) = mex(\{\emptyset\}) = 0$
- *Pilha com* 1 *feijão,* $g(1) = mex(\{g(0)\}) = mex(\{0\}) = 1$
- *Pilha com* 2 *feijões,* $g(2) = mex(\{g(1)\}) = mex(\{1\}) = 0$
- *Pilha com* 3 *feijões,* $g(3) = mex(\{g(2)\}) = mex(\{0\}) = 1$
- *Pilha com* 4 *feijões,* $g(4) = mex(\{g(3), g(0)\}) = mex(\{1,0\}) = 2$
- *Pilha com* 5 *feijões,* $g(5) = mex(\{g(4), g(1)\}) = mex(\{2,1\}) = 0$
- *Pilha com* 6 *feijões,* $g(6) = mex(\{g(5), g(2)\}) = mex(\{0,0\}) = 1$

- *Pilha com* 7 *feijões,* $g(7) = mex(\{g(6), g(3)\}) = mex(\{1, 1\}) = 0$
- *Pilha com* 8 *feijões,* $g(8) = mex(\{g(7), g(4)\}) = mex(\{0, 2\}) = 1$
- *Pilha com* 9 *feijões,* $g(9) = mex(\{g(8), g(5)\}) = mex(\{1, 0\}) = 2$
- *Pilha com* 10 *feijões,* $g(10) = mex(\{g(9), g(6)\}) = mex(\{2, 1\}) = 0$

$$\vdots$$

Por forma a organizar os dados, formalizamos uma tabela, assim:

n	0	1	2	3	4	5	6	7	8	9	10	...
$g(n)$	0	1	0	1	2	0	1	0	1	2	0	...

Portanto, se o jogo tiver apenas uma pilha, a estratégia é deixar um múltiplo de 5 *ou ainda um múltiplo de* 5 *mais* 2.

Contudo, se houver diversas pilhas, por exemplo, se o jogo começa com pilhas de 3, 6, 9 *e* 10 *feijões, então a posição* $P = (3, 6, 9, 10)$ *terá o nímero,*

$$g(P) = g(3) \oplus g(6) \oplus g(9) \oplus g(10) = 1 \oplus 1 \oplus 2 \oplus 0 = 2.$$

Assim, a estratégia vencedora consiste em subtrair 2 *(ou somar* 2*) de alguma das pilhas. Uma das formas para obtê-la, é reduzir a pilha de* 9 *feijões para* 5 *(pois g(5)=0); e, ainda, outra forma é trocar g(10)=0 por g(9)=2, ou seja, reduzir a pilha de* 10 *para* 9.

Exemplo 4.3.11 : *Novamente um jogo Nim, mas agora o conjunto de possíveis retiradas é* 2, 4 *e* 7. *Vamos ter para uma pilha de* 0 *a* 1 *feijões, a* $g(n) = 0$, *enquanto para as seguintes, temos:*

- $g(2) = mex(\{g(0)\}) = mex(\{0\}) = 1$
- $g(3) = mex(\{g(1)\}) = mex(\{0\}) = 1$
- $g(4) = mex(\{g(2), g(0)\}) = mex(\{1, 0\}) = 2$
- $g(5) = mex(\{g(3), g(1)\}) = mex(\{1, 0\}) = 0$
- $g(6) = mex(\{g(4), g(2)\}) = mex(\{2, 1\}) = 1$

- $g(7) = mex(\{g(5), g(3), g(0)\}) = mex(\{2, 1, 0\}) = 3$
- $g(8) = mex(\{g(6), g(4), g(1)\}) = mex(\{0, 2, 0\}) = 1$
- $g(9) = mex(\{g(7), g(5), g(2)\}) = mex(\{3, 2, 1\}) = 0$
- $g(10) = mex(\{g(8), g(6), g(3)\}) = mex(\{1, 0, 1\}) = 2$
- $g(11) = mex(\{g(9), g(7), g(4)\}) = mex(\{0, 3, 2\}) = 1$
- $g(12) = mex(\{g(10), g(8), g(5)\}) = mex(\{2, 1, 2\}) = 0$
- $g(13) = mex(\{g(11), g(9), g(6)\}) = mex(\{1, 0, 0\}) = 2$

$\vdots$

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	...
$g(n)$	0	0	1	1	2	2	0	3	1	0	2	1	0	2	...

De facto, $g(n)$ *inicia-se um pouco desordenada, mas acaba por ficar periódica com um conjunto de algarismos* (102) *a partir daí. Assim, com apenas uma pilha, a estratégia é deixar sempre* 1 *ou um múltiplo de* 3 *para o adversário, mas não exatamente* 3*! E, ainda, por exemplo, se houver* 5, 7 *ou* 10 *feijões na pilha, a estratégia é deixar* 1, 0 *ou* 6*, respetivamente!*

Porém, se houver várias pilhas, por exemplo, se o jogo começa com pilhas de 4, 7, 9, 10 *e* 13 *feijões, então a posição* $P = (4, 7, 9, 10, 13)$ *terá o nímero,*

$$g(P) = g(4) \oplus g(7) \oplus g(9) \oplus g(10) \oplus g(13) = 2 \oplus 3 \oplus 0 \oplus 2 \oplus 2 = 1.$$

Assim, a estratégia vencedora consiste em subtrair 2 *(ou somar* 2*) de alguma das pilhas. Uma das formas para obtê-la, é reduzir a pilha de* 9 *feijões para* 2 *(pois g(2)=1); outra forma é trocar g(7)=3 por g(5)=2, ou seja, reduzir a pilha de* 7 *para* 5*.*

4.3.2 O Jogo Kayles

O jogo Kayles (ver [3, 8]) é um jogo de boliche que começa com n pinos dispostos numa fila de pinos adjacentes. Cada jogador, jogando alternadamente, pode, em cada jogada, acertar num único pino ou em dois pinos adjacentes, possivelmente, quebrando uma fila em duas, ou diminuindo uma fila.

Após cada jogada, ficará um certo número de filas de pinos adjacentes. Deste modo e, depois da primeira jogada, obtemos ou uma fila com $n-1$ ou $n-2$ pinos, ou duas filas com tamanhos a e b, em que $a+b=n-1$ ou $a+b=n-2$, sendo as filas com 0 pinos ignoradas. De salientar que não é permitido aos jogadores derrubar dois pinos que não sejam adjacentes. O jogador perde o jogo se não puder derrubar mais pinos, ou seja, vence o jogo quem derrubar o último pino. Designamos uma fila de n pinos adjacentes por K_n, e uma posição de duas filas de a e b pinos por $K_a + K_b$. (De referir que em vez de denotarmos $K_a + K_0$ designaremos somente K_a).

Apresentamos, de seguida, para o jogo Kayles a seguinte definição:

Definição 4.3.12 (Função de Sprague-Grundy associada ao jogo Kayles). *Dado o jogo Kayles, a* função de Sprague-Grundy $g(K_n)$ *associada a este jogo, que a cada posição K_n do jogo, associa um número da posição K_n, é definida,*

$$g(K_n) = \text{mex}\{g(K_a + K_b) : a+b = n-1 \ \ ou \ \ a+b = n-2\}, \tag{4.2}$$

onde K_n representa n pinos adjacentes.

Pela proposição 4.3.8, temos $g(K_a + K_b) = g(K_a) \oplus g(K_b)$.

Exemplo 4.3.13 : *Consideremos o jogo Kayles no seu decurso, onde temos filas de tamanhos* 1, 7 *e* 3. *Verifiquemos a função de Sprague-Grundy $g(K_n)$ associada a este jogo, que a cada posição K_n do jogo, associa o número da posição K_n, definida em (4.2):*

- $g(K_0) = \text{mex}(\emptyset) = 0$
- $g(K_1) = \text{mex}(\{g(K_0)\}) = \text{mex}(\{0\}) = 1$
- $g(K_2) = \text{mex}(\{g(K_1), g(K_0)\}) = \text{mex}(\{1,0\}) = 2$
- $g(K_3) = \text{mex}(\{g(K_2), g(K_1), g(K_1) \oplus g(K_1)\}) = \text{mex}(\{2,1,1\oplus 1\}) =$
  $= \text{mex}(\{2,1,0\}) = 3$
- $g(K_4) = \text{mex}(\{g(K_3), g(K_2), g(K_1) \oplus g(K_2), g(K_1) \oplus g(K_1)\}) =$
  $= \text{mex}(\{3,2,1\oplus 2,0\}) = \text{mex}(\{3,2,3,0\}) = 1$
- $g(K_5) = \text{mex}(\{g(K_4), g(K_3), g(K_1) \oplus g(K_3), g(K_1) \oplus g(K_2), g(K_2) \oplus g(K_2)\}) =$
  $= \text{mex}(\{1,3,1\oplus 3, 1\oplus 2, 0\}) = \text{mex}(\{1,3,2,3,0\}) = 4$

- $g(K_6) = \text{mex}(\{g(K_5), g(K_4), g(K_1) \oplus g(K_4), g(K_1) \oplus g(K_3), g(K_2) \oplus g(K_3), g(K_2) \oplus g(K_2)\}) = \text{mex}(\{4, 1, 0, 1 \oplus 3, 2 \oplus 3, 0\}) = \text{mex}(\{4, 1, 0, 2, 1, 0\}) = 3$

- $g(K_7) = \text{mex}(\{g(K_6), g(K_5), g(K_1) \oplus g(K_5), g(K_1) \oplus g(K_4), g(K_2) \oplus g(K_4), g(K_2) \oplus g(K_3), g(K_3) \oplus g(K_3)\}) = \text{mex}(\{6, 5, 1 \oplus 5, 1 \oplus 3, 1 \oplus 4, 2 \oplus 4, 2 \oplus 3, 0\}) = = \text{mex}(\{6, 5, 4, 5, 6, 1, 0\}) = 2$

$$\vdots$$

Portanto, a posição $K_1 + K_7 + K_3$ tem o nímero

$$g(K_1 + K_7 + K_3) = g(K_1) \oplus g(K_7) \oplus g(K_3) = 1 \oplus 2 \oplus 3 = 0.$$

Podemos verificar a função de Sprague-Grundy para o Jogo Kayles (ver [3])

$$g(n)^{4} = g(n \mod 12),$$

para todos os valores de n com exceção dos seguintes:

$$g(0) = 0; g(3) = 3; g(6) = 3; g(9) = 4; g(11) = 6; g(15) = 7; g(18) = 3;$$

$$g(21) = 4; g(22) = 6; g(28) = 5; g(34) = 6; g(39) = 3; g(57) = 4; g(70) = 6.$$

Assim, para os valores de n, temos os seguintes valores nímericos para o jogo Kayles:

$$g(0 \mod 12) = 4; \quad g(4 \mod 12) = 1; \quad g(8 \mod 12) = 1;$$

$$g(1 \mod 12) = 1; \quad g(5 \mod 12) = 4; \quad g(9 \mod 12) = 8;$$

$$g(2 \mod 12) = 2; \quad g(6 \mod 12) = 7; \quad g(10 \mod 12) = 2;$$

$$g(3 \mod 12) = 8; \quad g(7 \mod 12) = 2; \quad g(11 \mod 12) = 7.$$

Para o jogo Kayles, qualquer que seja o número de pinos considerado, podemos também determinar uma estratégia vencedora, conforme mostramos no próximo resultado.

[4] Para simplificar a escrita, substituiu-se k_n por n.

Teorema 4.3.14 *No jogo Kayles com n filas com $p_1, \ldots, p_n$ pinos existe uma estratégia vencedora para o jogador que começa o jogo a partir de uma certa posição se e só se o nímero dessa posição for maior ou igual a* 1.

Podemos encontrar a demonstração deste resultado em [14].

Exemplo 4.3.15 : *Consideremos o jogo Kayles com uma fila de* 10 *pinos adjacentes. Denotemos por K_{10} a fila de* 10 *pinos adjacentes. Pela definição 4.2, temos $g(K_{10}) = 2$. Portanto, uma D-posição.*

O jogador que começa o jogo a partir desta posição transforma-a numa V-posição, da seguinte forma: derruba 2 *pinos adjacentes ao meio da fila transformando a posição K_{10} em $K_4 + K_4$. Assim, para a posição $K_4 + K_4$ temos*

$$g(K_4 + K_4) = g(K_4) \oplus g(K_4) = 1 \oplus 1 = 0.$$

Portanto, a posição $K_4 + K_4$ é uma V-posição.

O jogador seguinte fará um movimento qualquer e transforma-la-á numa D-posição, por exemplo, a uma das posições K_4 se derrubar 1 *pino obtém a posição K_3. Assim, passamos a ter a posição $K_3 + K_4$, sendo $g(K_3 + K_4) = g(K_3) \oplus g(K_4) = 3 \oplus 1 = 2$.*

Portanto, a posição $K_3 + K_4$ é uma D-posição.

Prosseguindo com jogadas para posições com soma-Nim nula, verificamos que o primeiro jogador vai ganhar o jogo.

Bibliografia

[1] Paulo J. Almeida, *Teoria dos Números e Aplicações*, Departamento de Matemática - Universidade de Aveiro, Notas 2012.

[2] Tom M. Apostol, *Introduction to Analytic Number Theory*, New York Springer, 1995.

[3] Elwy R. Berlekamp, J. H. Conway, Richard K. Guy, *Winning ways for your mathematical plays*, A K Peters, Natick, MA, USA, 2001, vol.1.

[4] Elwy R. Berlekamp, J. H. Conway, Richard K. Guy, *Winning ways for your mathematical plays*, A K Peters, Natick, MA, USA, 2001, vol.2.

[5] Elwy R. Berlekamp, J. H. Conway, Richard K. Guy, *Winning ways for your mathematical plays*, A K Peters, Natick, MA, USA, 2001, vol.3.

[6] H.L. Bodlaender, D. Kratsch, *Kayles and Nimbers*, Journal of Algorithms, 43, 2002, 106-119.

[7] Charles L. Bouton, Nim, a game with a complete mathematical theory, *Ann. Math.* 3, 1902, 35-39.

[8] John H. Conway, *Os números e os jogos*, Gradiva, 2010.

[9] John H. Conway, Richard K. Guy, *O livro dos números*, Gradiva, 1999.

[10] Jean-Paul Delahaye, *Merveilleux nombres premiers : voyage au coeur de l'arithmetique*, Berlin, 2000.

[11] Thomas. S. Ferguson, *Game theory*, Departamento de Matemática da Universidade da Califórnia, Los Angeles, 2005.

[12] Brian. D. Ginsberg, *Midy's (Nearly) Secret Theorem - An Extension After 165 Years*, College Mathematics Journal, 35, 2004, 26-30.

[13] Rashmi Gupta, M. R. Murty, *A remark on Artin's Conjecture*, Inventiones Math n. 78, 127-130, 1984.

[14] Richard K. Guy, C. A. B. Smith, *The G-values of various games*, Proc. Cambridge Philos, Soc., 52:514-526, 1956.

[15] Harold G. Hardy, Edward M. Wright, *An introduction to the theory of numbers*, 5a edição, Clarendon Press, Oxford, 1979.

[16] William G. Leavitt, *A Theorem on repeating decimals*, Department of Mathematics - University of Nebraska, 1967.

[17] H. W. Lenstra, Jr., *Nim multiplication*, Séminaire de Théorie des Nombres, N. 11, Université de Bordeaux, 1977.

[18] Joseph Lewittes, *Midy's Theorem for Periodic Decimals*, Integers: Electronic Journal of Combinatorial Number Theory, 7, 2007.

[19] Harold W. Martin, *Generalizations of Midy's Theorem on repeating Decimals*, Integers: Electronic Journal of Combinatorial Number Theory, 7, 2007.

[20] Vítor Neves, *Introdução à Teoria dos Números*, Departamento de Matemática - Universidade de Aveiro, Notas 2006.

[21] Paulo A. J. Oliveira, *O teorema de Fermat-Euler-Silva*, Boletim da Sociedade Portuguesa de Matemática n. 45, 65-72.i

[22] Brígida A. Sartini et al., *Uma introdução à teoria de jogos*, II Bienal da SBM. Universidade Federal da Bahia (25 a 29 de outubro), 2004.

[23] Jorge N. Silva, *Jogos matemáticos*, Auditório Municipal de Óbidos (7 de junho), Notas 2003.

[24] Jorge N. Silva, J. P. Neto, *Jogos matemáticos, jogos abstractos*, Biblioteca Desafios Matemáticos, RBA Coleccionables. Barcelona, 2008.

[25] Gérard Villemin, *Nombre Tetu* (página consultada em janeiro de 2013), http://villemin.gerard.free.fr/Wwwgvmm/Nombre/Tetu.htm

[26] Eric W. Weisstein, *Euler's Totient Rule* (página consultada em abril de 2013), http ://mathworld.wolfram.com/MidysTheorem.html

[27] WIKIPEDIA, *Ciclic Number* (página consultada em setembro de 2013), http://en.wikipedia.org/wiki/Cyclicnumber

[28] WIKIPEDIA, *Parasitic Number* (página consultada em setembro de 2013), http://en.wikipedia.org/wiki/Parasiticnumber